‘Lake Dale Contact Centre’ Case Study

This section contains the Case Study information for a fictitious organization called “Lake Dale Contact Centre (LDCC).”

Please note that the documents included in this Case Study contain errors for training purposes only. These documents should not be used as guides for developing management system documentation.

******ASSUME THE CURRENT MONTH IS NOVEMBER FOR THE PURPOSE OF YOUR AUDITS AND RECORDS INSPECTION******

Case Study Table of Contents

…making excellence a habit.™

MASTER DOCUMENT CONTROL FORM – MDC01 – Issue 1

This Form applies to all policies, processes, procedures, forms, protocols and similar documents, produced by Lake Dale Contact Centre (LDCC), that need to be controlled within the Information Security Management System (ISMS). This is to ensure a consistent approach: in that only the most up to date version of any document is available, online at any point in time, and to ensure that documents are relevant, concise and current.

Document Number	**Issue status**	**Document Category and location/responsibility**	**Retention time (years)**
MDC01	1	Operations Manager	Until revised
MDC02	1	Operations Manager	Until revised
D1	3	MD/CEO	*(Until not needed)*
D2	3	MD/CEO	‘ ’
D3	1	MD/CEO	‘ ’
D4	1	MD/CEO	‘ ’
D5	1	MD/CEO	‘ ’
D5	1	MD/CEO	‘ ’
D6	2	MD/CEO	‘ ’
D7	1	MD/CEO	‘ ’
D8	1	IS Manager/Management representative for ISMS	‘ ’
D9	1	IS Manager/Management representative for ISMS	‘ ’
D10	1	IS Manager/Management representative for ISMS	‘ ’
D11	1	IS Manager/Management representative for ISMS	‘ ’
D12	3	IS Manager/Management representative for ISMS	‘ ’
D13	1	IS Manager/Management representative for ISMS	‘ ’
D14	1	IS Manager/Management representative for ISMS	‘ ’
D15	1	IT Manager	‘ ’
D16	2	IS Manager	‘ ’
D17	2	MD/CEO	‘ ’
D18	3	HR Director	‘ ’
D19	3	HR Director	‘ ’
D20	1	HR Director	‘ ’
D21	1	Team Leader/IT Manager	‘ ’
D22	1	Receptionist	‘ ’
D23	1	IT Manager	‘ ’
D24	3	Analyst/Systems Admin	‘ ’
D25	2	Facilities Manager	‘ ’
D26	1	Facilities Manager	‘ ’
D27	1	Finance Director	‘ ’
D28	1	Receptionist	‘ ’
D29	1	HR Director	‘ ’
D30	2	MD/CEO	‘ ’
D31	1	MD/CEO	‘ ’
D32	1	HR Manager	‘ ’
D33	2	HR Director	‘ ’
D34	1	HR Director	‘ ’

D35	1	HR Director	‘ ’
D36	2	HR Manager	‘ ’
D37	3	MD/CEO	‘ ’
D38	2	MD/CEO	‘ ’
D39	1	IS Manager/Management representative for ISMS	‘ ’
D40	1	Controls Manager/ISMS Auditor	‘ ’
D41	1	Team Leader/IT Manager	‘ ’
D42	3	Controls Manager/ISMS Auditor	‘ ’

Master Document Change Request Form – MDC02 – Issue 1

SECTION A – PROPOSER

Requested by:		**Date:**		
Department:		**Ext:**		
Change				
	Current reference of document(s) to be changed/withdrawn	**Issue status**	**Date**	**Change Required**
Proposal to **issue new** document(s)				
Proposal to **change** document(s)				
Proposal to **withdraw** (document(s)				
Details of proposal/change (attach relevant document(s))				

SECTION B : PROCEDURE OWNER

Request accepted / not accepted (delete as appropriate)

Signed: **Date**:

SECTION C : PROCEDURE AUTHORISER

Request approved / not approved (delete as appropriate)

Signed: **Date**:

...making excellence a habit.™

SECTION D : DOCUMENT CONTROLLER

New document reference: Issue : Date:

New master document received: □

Document distributed to users by document controller □

Procedures register updated □

Signed: ________________________________ **Date:**____________________

Strategic Mission Statement – D1 – Issue 3

LDCC is a call centre specialist that provides very high quality, price-competitive customer contact solutions on behalf of numerous multinational and blue chip companies. Our 150 seat call centre is state of the art and provides our staff with a clean, modern and inspiring place to work. We offer Finance, Personnel, Utilities and Sales services.

Our overall strategic mission is to provide our clients with:

- an outsourced service including technical infrastructure, process expertise and management experience, but at a lower cost and without long term contract commitment
- the highest degree of integrity, professionalism and information security from our own outsourced providers
- a secure environment and best practice that conforms to ISO 27002 and ISO 9001
- business continuity, so ensuring the availability of data
- information security for the data integrity we retain and that provided

Information Security Policy – D2 – Issue 2

This policy has been developed by the Management Information Security Forum (ISF)

The ISF are committed to satisfying applicable requirements relating to Information Security and are committed to continual improvement of the Information Security.

The organization places great emphasis on the need for the strictest confidentiality in respect of client data. This applies to manual and computer records and telephone conversations. The organisation will strive to improve its confidentiality processes in respect to client data.

We will control or restrict access so that only authorised individuals and partners can view sensitive information. Access to client information is limited only to those individuals and partners who have a specific need to see or use that information.

Information will not be made available to outside parties without the written consent of the information owners.

We are committed to meeting all Information Security requirements from our customers and the provision of the necessary resources.

We are committed to encouraging Information Security improvements by engaging with our workforce.

This policy will be implemented through a recognised Information Security Management System that has been self-declared by the ISF.

Approved by:

Clive Prichard IS Manager

Scope Statement

The Information Security Management System (ISMS) applies to the provision of telephony services, the management of information and business support services at our only site in Mumbai (India), in accordance with the ISMS Statement of Applicability revision 03, dated 21/Sept/20xx. The scope of this ISMS excludes all IS outsourced processes (as these are not controlled by LDCC).

Roles and Responsibilities – D3 – Issue 1

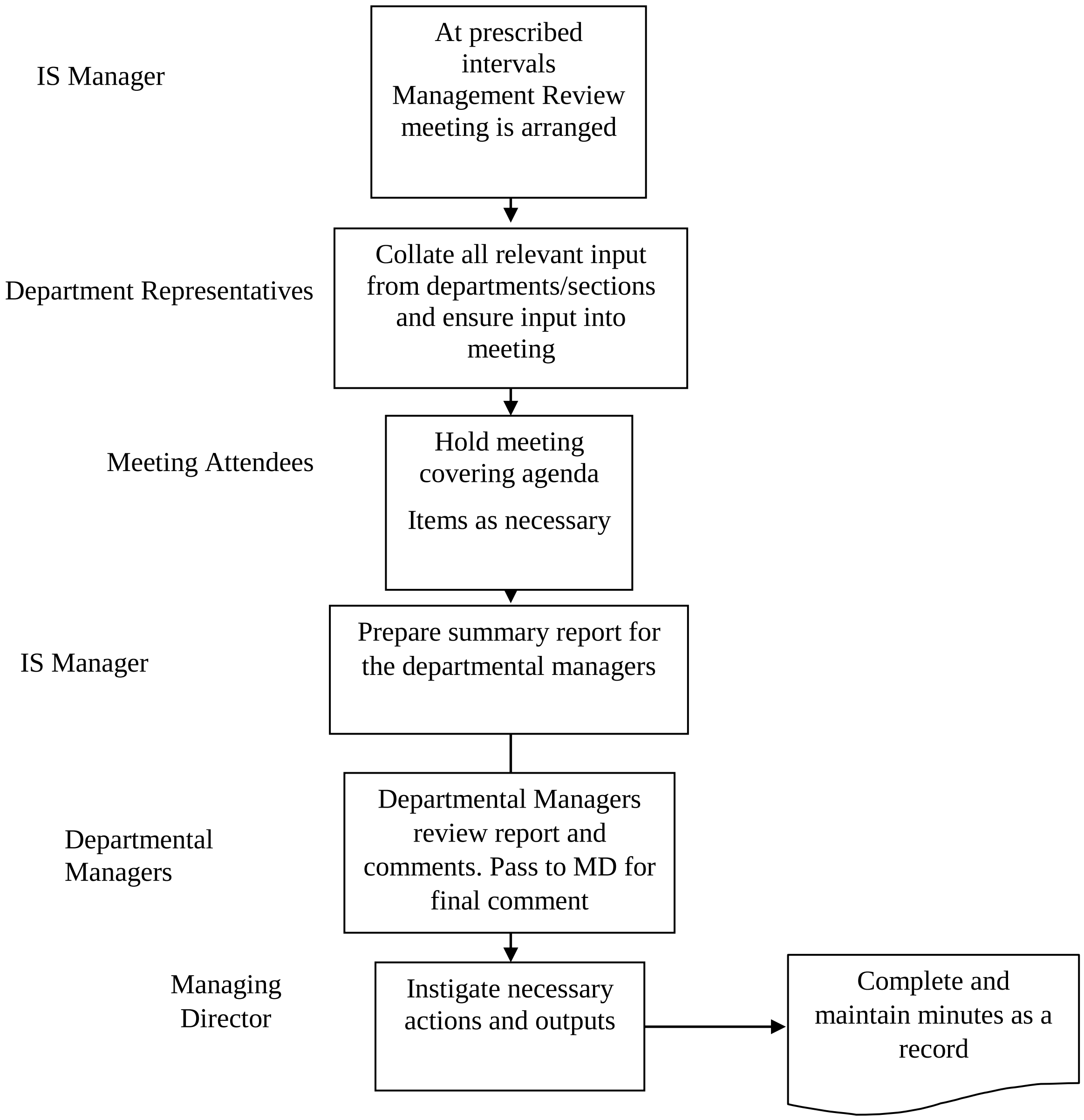
Management System Owner - Managing Director	1. ensuring the integration of the information security management system requirements into the organization's processes; 2. ensuring that the resources needed for the information security management system are available; 3. communicating the importance of effective information security management and of conforming to the information security management system requirements; 4. ensuring that the information security management system achieves its intended outcome(s); 5. directing and supporting persons to contribute to the effectiveness of the information security management system; 6. promoting continual improvement; and 7. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. 8. assign responsibility and authority for the ISMS Representative below
ISMS Management Representative	1. ensuring that the information security management system conforms to the requirements of this International Standard; and 2. reporting on the performance of the information security management system to top management
ISF Members (rotating membership - see management review records)	1. defining risk and opportunities planning process 2. define the ISMS process 3. define the IS risk treatment process 4. approving the ISMS activities undertaken 5. reviewing of incidents and corrective actions 6. reviewing of information security audit reports
ISMS Auditor	1. Planning of ISMS Audit Schedule 2. Undertaking audits and monitoring progress 3. Reporting to the ISF

Operations Manager	1. Management of assets 2. Asset register ownership 3. Manage budgets and other documentation 4. Perform training sessions
Tele Manager	1. Ensuring telephone staff follow policies
All Phone operatives	1. Follow policies and directions
HR Manager	1. Protection of HR records 2. Staff vetting and background checks
Janitor/Cleaners	1. Collection of printed paper waste 2. Disposal of sensitive information
IT Team leader	1. Physical protection of IT infrastructure 2. Logical protection of data and IT access
Receptionist	1. Physical protection 2. Visitor, staff badging

Management Review Process – D4 – Issue 1

Meeting attendees, where possible:

- IS Manager (Management Representative for ISMS)
- Operations Manager
- Sales Manager
- Tele Manager & IT Manager
- Finance Manager
- Facilities Manager
- (Other personnel as required)


IS Manager
At prescribed intervals Management Review meeting is arranged
Department Representatives
Collate all relevant input from departments/sections and ensure input into meeting
Meeting Attendees
Hold meeting covering agenda
Items as necessary
IS Manager
Prepare summary report for the departmental managers
Departmental Managers
Departmental Managers review report and comments. Pass to MD for final comment
Managing Director
Instigate necessary actions and outputs
Complete and maintain minutes as a record

MANAGEMENT SYSTEM REVIEW MINUTES

18th January 20xx

Management System Review Minutes – D5 – Issue 1

Attendees: Clive Page (CPa) – Sales Manager
Gordon Black (GB) – Controls Manager
Amanda French (AF) – Operations Manager
Philip Hernshaw Smyth (PHS)– Accounts Manager
Clive Pritchard (CPr) – IS Manager
Simon Lock (SL) - Facilities Manager

Apologies: Rodney Trotter (Philip Hernshaw Smyth attended in his place)

Objectives

The purpose of this management review was to review the LLDC Information Security Management System and address possible needs for changes in the policy, objectives and other elements of the Management System, in light of audit results, changing circumstances and the company's commitment to continual improvement.

1 Results from previous ISMS audits and reviews

Audit results seem to indicate an area of weakness around 'integrity' loss of customer data. Also staff have reported problems gaining access to information that they are authorized to view.

2 Techniques, products and procedures which could be used in the organisation to improve the ISMS performance and effectiveness

Our Fire Wall is a disgrace; with IT Staff regularly reporting they can hack our systems from home.

Objective now in place for this, so no worries here.

3 Status of nonconformities and corrective actions

As nonconformities only arise from IS incidents, or audits, they are recorded in the corrective action log and managed through that process. No need to look at this again here.

4 Results of risk assessment and status of risk treatment plans.

The risk assessment gives us levels of acceptable risk. This has been approved by the ISF. There have been no changes in the business that would suggest that these levels need changing at the moment.

5 Vulnerabilities or threats not adequately addressed in the previous risk assessment

None

6 Follow up actions from previous management reviews

All outstanding actions have been implemented and verified by the ISF.

7 Any changes to internal or external issues that could affect the ISMS

Increasing staff levels, now reaching 150: cannot keep upto date with the screening process – need to keep our customer’s happy; so a concession has been granted, by the ISF to HR, allowing discretion in whom to screen.

8 Recommendations for improvement:

A. Undertake penetration tests of building and IT systems to verify concerns and support the objective budget
B. Need more trained internal auditors; as the one we have is leaving shortly.

9 Lessons from incidents

No incidents have been reported as yet, this situation is likely to change as more staff undertake the induction awareness training.

10 Fulfilment of information security objectives

Covered separately in the reviews for each objective (please see objectives).

11 Actions arising from the review:

1. Ensure that all new staff have attended an awareness session on IS (induction)

12 Next planned review: To be determined

Final comments from MD: ……………………………………………………………………………………………………

MD Signed……..Mr Swan……….

MANAGEMENT SYSTEM REVIEW MINUTES

16th October 20xx

Management System Review Minutes – D5 – Issue 1

Attendees: Clive Page (CPa) – Sales Manager

Lauren Hunter (LH) – Receptionist

Kate Lough (KL) – Phone Operative

Reggie Gates (RG) – Phone Operative

Sarah Wallmarsh – (SW) – Janitor/Cleaner

Apologies: Gordon Black (GB) – Controls Manager

Amanda French (AF) – Operations Manager

Philip Hernshaw Smyth (PHS) – Accounts Manager

Clive Pritchard (CPr) – IS Manager

Simon Lock (SL) - Facilities Manager

Objectives

The purpose of this management review was to review the LLDC Information Security Management System and address possible needs for changes in the policy, objectives and other elements of the Management System, in light of audit results, changing circumstances and the company’s commitment to continual improvement.

1 Results from previous ISMS audits and reviews

Audits were reduced when Gordon Black left the organization in March. Really need to secure a permanent resource. Audits are currently being shared out amongst phone operatives in quiet periods, which they are not happy with.

2 Techniques, products and procedures which could be used in the organisation to improve the ISMS performance and effectiveness

Visitors have been reported walking around observing and listening to phone operatives conversations. Friends of staff have also been observed using security passes to access our site. On one occasion an ex-employee was observed at his old desk talking to a new member of staff that replaced him. This should all be rectified now with the new access control procedure.

3 Status of nonconformities and corrective actions

As nonconformities only arise from IS incidents, or audits, they are recorded in the corrective action log and managed through that process. No need to look at this again here.

4 Results of risk assessment and status of risk treatment plans.

There was no-one in the meeting that knew anything about this - too technical. We will leave this to the IT Manager.

5 Vulnerabilities or threats not adequately addressed in the previous risk assessment

None

6 Follow up actions from previous management reviews

Not reviewed in this meeting (as different attendees).

7 Any changes to internal or external issues that could affect the ISMS

Increasing competition and wage demands from our phone operatives now; as competitors have moved near us, competing for our customer's and staff. HR informed the Sales Manager, before this meeting, that an increase in our staff turnover (churn rate) was now evident and a real concern for us. Termination of employment controls therefore needs auditing and bolstering up to meet this risk.

8 Recommendations for improvement:

C. Security Guard is very rude when checking our passes upon entering the building (he needs a personality test)
D. Need more trained internal auditors; as the one we had has left and phone operatives are not happy covering for this during their tea break.

9 Lessons from incidents

No incidents have been reported to the ISF for review.

10 Fulfilment of information security objectives

Covered separately in the reviews for each objective (please see objectives).

11 Actions arising from the review:

1. Ensure security guard undergoes a personality test and recruit a new internal auditor.

12 Next planned review: To be determined

Final comments from MD: ……Not agreed…………………………………………………

MD Signed……..……….

Context

Security Context – D6 – Issue 2

The **purpose** of this organization is covered in: ‘Lake Dale Contact Centre (LDCC) – Strategic Mission Statement’.

Below are the external and internal issues that are relevant to LDCC’s purpose, in order to achieve the intended outcomes (policy) of its ISMS.

External issues relevant to the above (for its ISMS).

Legal and regulatory.

LDCC recognize there are legal and regulatory requirements over and above the requirements as established by our internal requirements.

Legislation	IS Requirements
1. Contract law	A contract is a legally enforceable exchange of promises. Any agreement we enter into must follow a set format or it could be invalid
2. Health & Safety Legislation	Legislation covering occupational health and safety in the UK is the Health and Safety at Work Act. It imposes general duties for health and safety on employers and employees. We must ensure the health, safety and welfare of all our employees

Cultural

11. Personal data - There is a known external demand for personal data (especially financial i.e. Credit card details, address details and dates of birth) and significant inducements can be offered to staff for the collection of information this could affect ‘confidentiality’.

12. Hacking and unauthorized interception of communications is an issue we know about targeting contact centers, this could affect ‘confidentiality’.

13. Wages in our industry are low and so bribery is an ever present threat, this could affect ‘confidentiality’.

Connectivity

14. Power and connectivity – utility failures are common and have occurred in the past. We have had power cuts due to local power demand increases that have interrupted mains power (new building and expanding businesses: the infrastructure cannot cope). IT connectivity has also been interrupted by this high demand. This could impact on ‘integrity’.

15. International clients are also expecting state of the art technology, fast connection speeds for sales and call handling report visibility (statistics). This has an impact on our commitments contained in our service level agreements.

Location

16. Physical location, our location is in an area of *high* criminality (due to many hi-tech businesses located nearby) and adjacent offices have been attacked by thieves which could have an impact on ‘confidentiality’.

17. Environmental – no particular flooding or storm damage is anticipated.

Competition

18. `Employees could take LDCC or customer information to a competitor. There are many competitors located close to our office. Staff can often move from our company to a competitor quickly. This could affect ‘confidentiality’.

Economic pressures

19. It is understood that when some of our competitors are under pressure for new revenue, they may be more likely to illicit sources of information on our customers from our key employees. This could also entail poaching key members of staff and securing access to confidential information. The loss of a key member of staff with the customer data they have access to could impact us heavily. This could affect ‘confidentiality’ and the viability of LDCC.

20. In tight financial times customers are seeking cost saving alternatives, we are therefore seeing a large increase in sales enquiries putting pressure on our internal resources and IT and IS systems.

Internal issues relevant to the above (for its ISMS).

Information systems

21. Some of our systems are old and due to be replaced. New systems will be more complex and possibly harder to support. Possible ‘integrity’ issues.

Organization’s culture

22. Historically our company has been sales driven, the need to bring in work has outweighed other considerations such as ‘confidentiality’. This has resulted in a misalignment between its strategic direction and IS policy. The integration of IS into the organization’s sales processes may not be strictly adhered to and top management support to demonstrate leadership in IS may be compromised when large orders are at stake.

Relationships and perceptions and values of internal stakeholders

23. Historically we have had high turnover in staff and this means staff could take data with them on departure. We understand that the skill sets of our call center staff are limited and as such documented processes and guidance are more important. Also comprehending the nature of IS policies and their importance and consequences may not be fully recognized and hence information security incidents are more likely.

24. Many skills and decision making authorities are restricted to a very few senior staff who know each other very well, this has led to a competence and documentation ‘gap’ through informality.

Human Resource Security and Capabilities (knowledge)

25. The high staff turnover has caused LDCC difficulties in retaining core knowledge, such as system support and customer relations. This may cause issues. Staff are recruited form the local workforce and because of the low wages and skills expectation they may not

be well off financially or well educated. This may leave them more vulnerable to bribery and corruption.

Governance, organization and roles and responsibilities

26. As a small company, responsibilities have been retained by a small management team. As we grow this may be difficult to achieve but is needed.

Standard working procedures and guides

27. Processes have not been documented because of their retention and ownership by senior individuals only. As we grow this lack of documentation may cause problems.

Contractual relationships with our suppliers

28. As a small new business our purchasing power and influence is restricted; as we are not able to include IS requirements in contracts, also some suppliers do not have formal contracts with us. Hence the scope of our ISMS excludes all IS outsourced processes. As ‘Data Cleansing’ is a current outsourced process, this naturally causes our clients concerns around ‘Confidentiality’ and ‘Integrity’.

Standards guidelines and models adopted by the organization

29. Top Management have decided not to seek certification to ISO 27001 nor to adopt all of its requirements, but are happy to commit to adopting the controls in ISO 27002 best practice.

Interested Parties – D7 – Issue 1

1. **Employees and their dependents**

   NA

2. **Partners**

   These may be agents or system partners, recruitment companies or others. Their reputations may be damaged if we have a breach, we may be damaged if they have a breach. Our contracts with some key partners may have or need IS clauses.

3. **Suppliers**

   Even a supplier may be affected by an incident, if our use of their systems results in negative publicity for the supplier they may not want to supply us. Data suppliers may not trust us with marketing lists.

4. **Insurers**

   If fines or damages were the result of an incident (breach of contract or regulator) this would affect profits and so investors and owners. Our insurer ‘may’ be liable to contribute depending on insurance wording.

5. **Government agencies**

   With recent government breaches, government departments have to be squeaky clean, they have not inspected us yet but may in the future. The governments IL2/3/4 requirements around IS may affect us if we take on that sort of work.

6. **Management/Shareholders**

   Breaches could affect our share price or our investors could withdraw. The professional reputation of the company and its management could be questioned if we had a breach.

7. **Media / Commentators**

   Interest in Information Security is growing, we should expect any incident to be reported and suffer bad publicity, perhaps suffering the loss of customers as a result.

8. **Regulators**

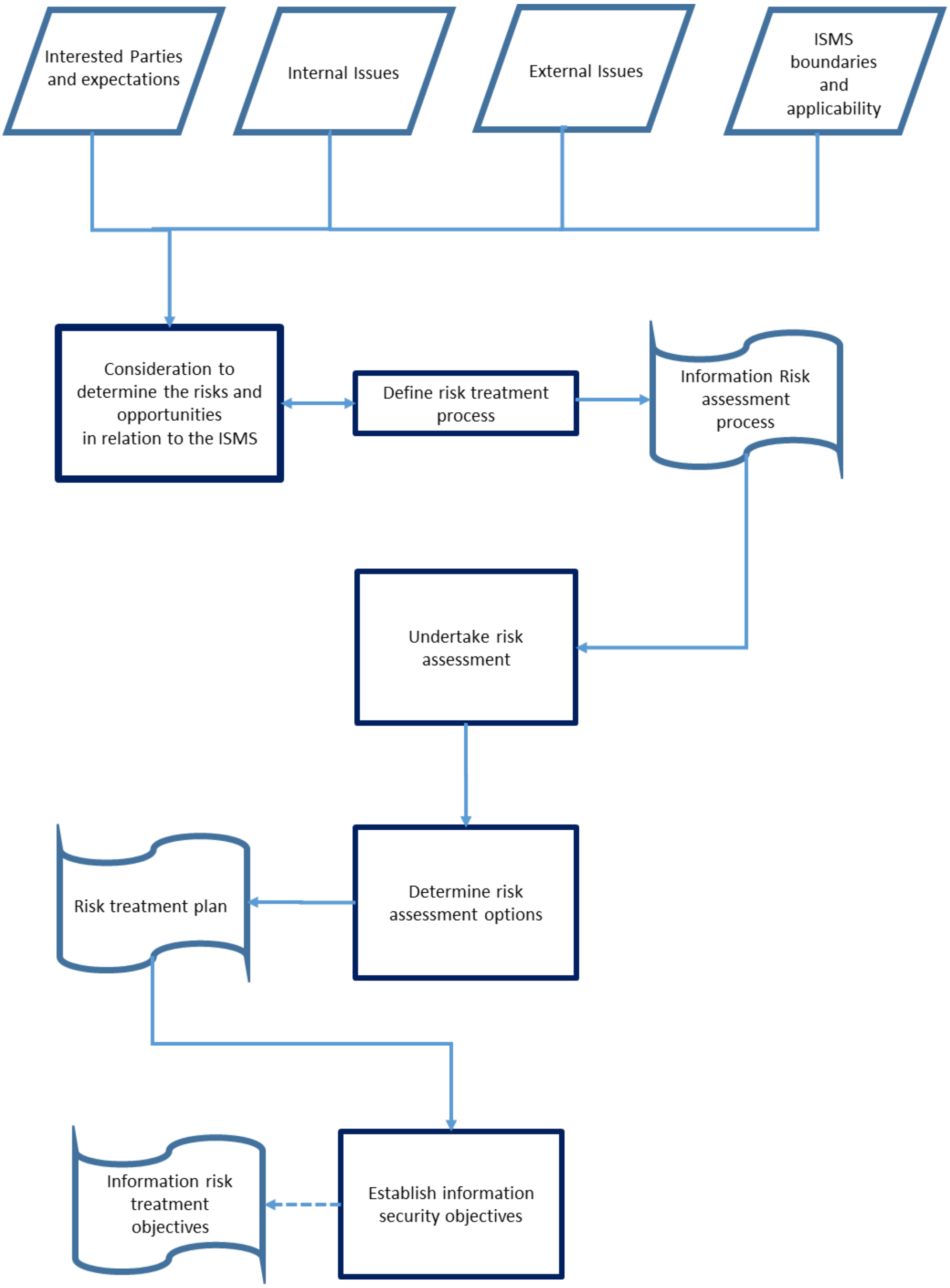
   Although we are not members of any regulated bodies we may seek to join at a later date. Organisations such as the Direct Marketing Association (DMA) have security requirements that we would need to follow.

9. **Law enforcement**

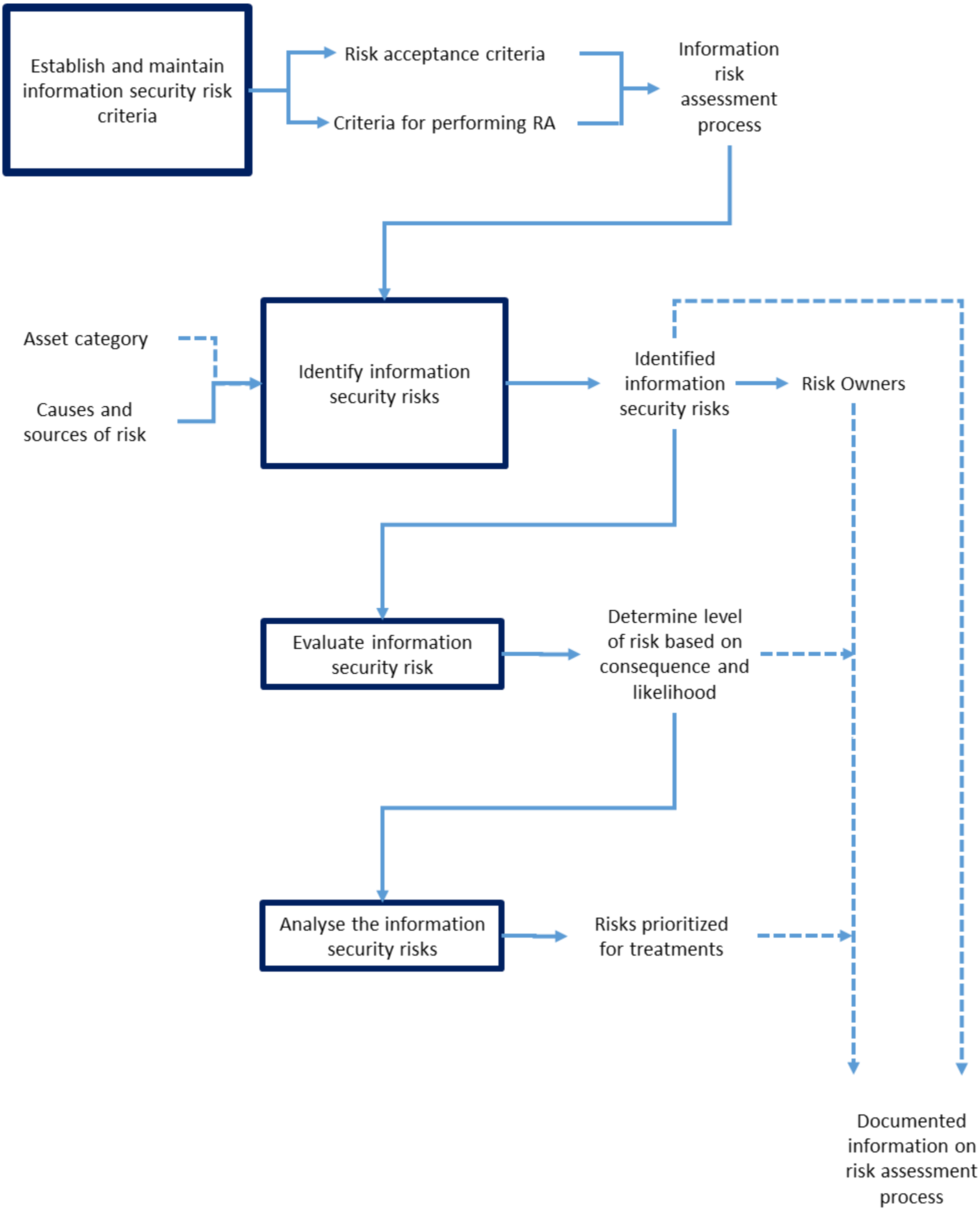
   If a breach broke the law we could be fined, face restrictions or directors face imprisonment.

Actions to Address Risks and Opportunities

Risk and Opportunities Planning Process – D8 – Issue 1

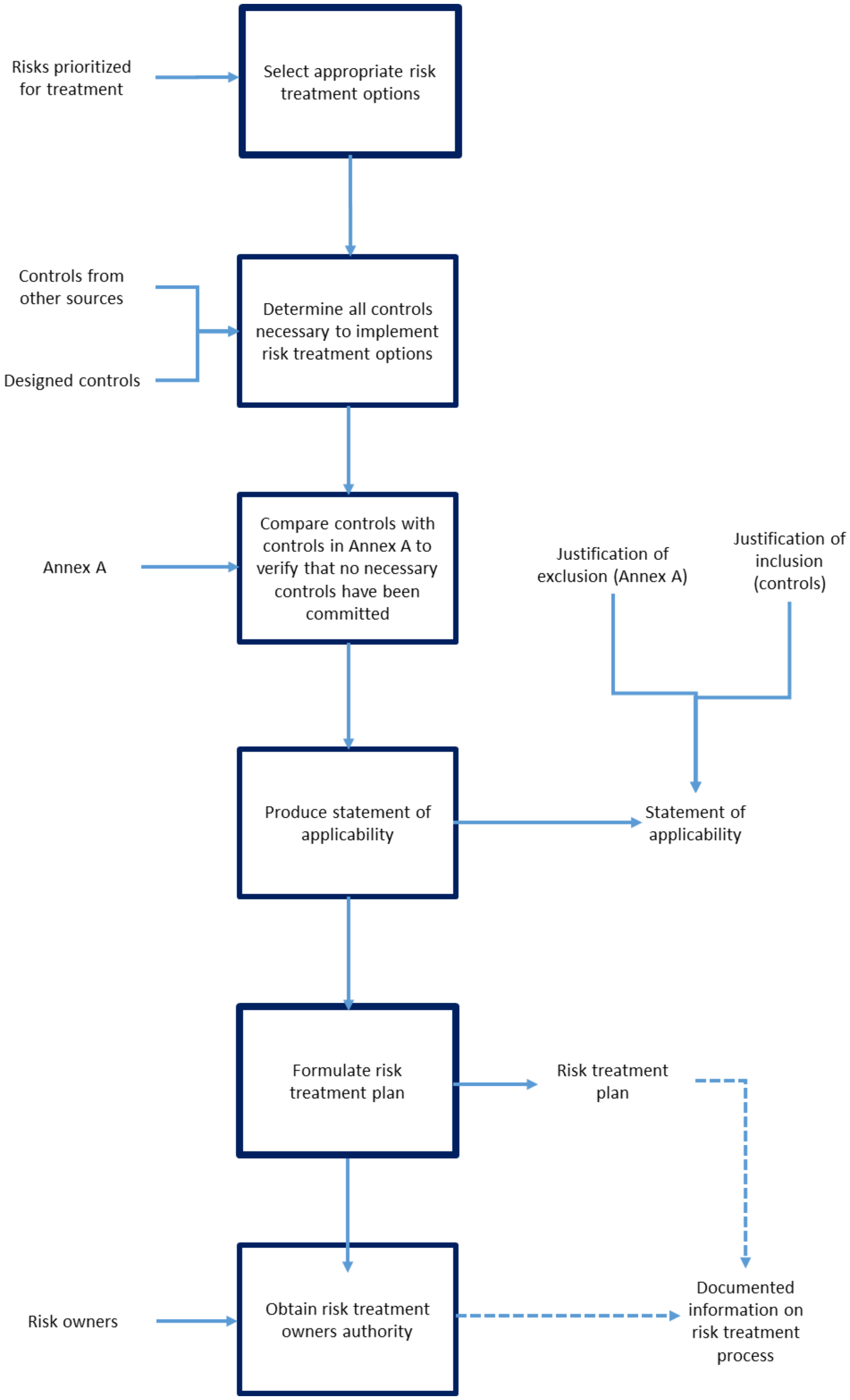

Interested Parties and expectations
Internal Issues
External Issues
ISMS boundaries and applicability
Consideration to determine the risks and opportunities in relation to the ISMS
Define risk treatment process
Information Risk assessment process
Undertake risk assessment
Determine risk assessment options
Risk treatment plan
Information risk treatment objectives
Establish information security objectives

Risk Assessment Process – D9 – Issue 1


Establish and maintain information security risk criteria
Risk acceptance criteria
Criteria for performing RA
Information risk assessment process
Asset category
Causes and sources of risk
Identify information security risks
Identified information security risks
Risk Owners
Evaluate information security risk
Determine level of risk based on consequence and likelihood
Analyse the information security risks
Risks prioritized for treatments
Documented information on risk assessment process

…making excellence a habit.™

Risk Treatment Process – D10 – Issue 1


Risks prioritized for treatment
Select appropriate risk treatment options
Controls from other sources
Designed controls
Determine all controls necessary to implement risk treatment options
Annex A
Compare controls with controls in Annex A to verify that no necessary controls have been committed
Justification of exclusion (Annex A)
Justification of inclusion (controls)
Produce statement of applicability
Statement of applicability
Formulate risk treatment plan
Risk treatment plan
Risk owners
Obtain risk treatment owners authority
Documented information on risk treatment process

Information Security Risk Procedure – D11 – Issue 2

Information Security Risk Criteria

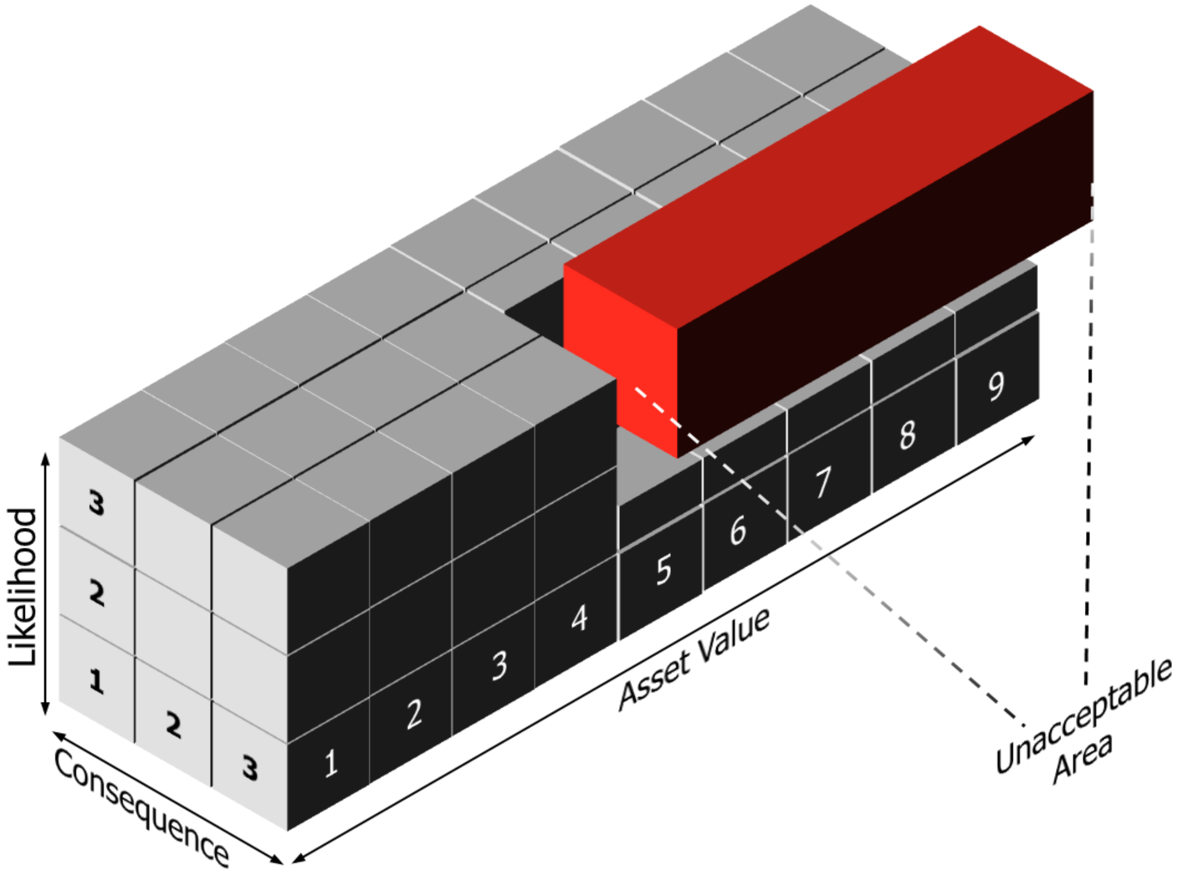
Performing IS Risk Assessments

The criteria for prompting a risk assessment will be:

1. Significant changes to the business affecting IS (determined by the ISF)
2. A new contract involving bespoke IS requirements (determined by the ISF)
3. After an Information Incident (single or series of unwanted or unexpected information security events – as agreed by the ISF)
4. A period not exceeding 3 years

IS Risk Acceptance Criteria

The criteria for IS risk acceptance is detailed below:



Any scores within the area indicated are to be categorised as unacceptable and prioritised as risk to be treated. Any scores outside the unacceptable area will not be prioritized for treated but however assessed for risk reduction in pursuit of continual improvement.

Identifying Information Security Risks

An inventory of asset groups will be created that reflect the information types held within LDCC.

These asset groups will be individually assessed for risk treatment as if they were singular assets. Any assets within each group, that needs to be assessed separately from the group, will be identified uniquely in the asset register.

Internal and external issues identified within the 'Context' and the specific requirements of our interested parties will be seen as asset groupings and risk assessed with opportunities identified, and treatment options considered.

Other risk sources, such as reported ARE events or incidents, will also be considered for risk assessment. This will be determined by the ISF at management review meetings.

For each asset identified a rating is give: on a scale from 1 – 3 for 'Confidentiality', 'Availability' and 'Integrity'. These values are added together to give an 'Asset Value'. Risk owners are identified at this point.

Analysing Information Security Risks

The potential consequences and realistic likelihood are determined, each on a scale of 1 – 3.

The 'Asset Value' identified above is now multiplied by the 'Consequence' and 'Likelihood' values to determine the level of risk for each asset (taking into account existing controls).

Evaluating Information Security Risks

Based on the 'Risk Acceptance Criteria' detailed above we have identified a score of over 40 as being the threshold for risk treatment (half of 81). These Information Security Risks will then be prioritised using a number score. The highest priority for risk treatment will be scores above 60 (these will left indented in the cell and identified as highest priority in the risk treatment plan). The next level of priority will be scores above 40 (these will centred in the cell and identified as medium priority in the risk treatment plan). Scores below 40 will not be prioritised for risk treatment (these will be right indented in the cell and if a risk treatment plan is created will be identified as lowest priority).

Information Security Risk Treatment

Once risks have been prioritised for treatment, one risk treatment option is chosen and identified. An Information Security (independent) consultant will be appointed to determine all controls from ISO 27002 that are necessary to implement the Information Security treatment options chosen. These controls will be identified, documented and kept up to date.

A Statement of Applicability will be created detailing controls selected and justification for inclusion.

Risk owner's acceptance of the residual Information Security risks will be documented.

An Information Security Risk Treatment Plan will be owned and held by the Information Security consultant.

	Information Asset	Details	Risk Owner
	GENERIC ASSETS		
Asset Register - D12 - Issue 3			
A1	Customer provided information	Our customers customer information in our systems, includes contact and financial information	To be determined shortly
A2	LDCC Customer contact Information	Our information on our customers	Sales Director
A3	LDCC Financial account information	Finance, invoicing, debts and bank	Finance Director
A4	LDCC HR Information	Wages, Next of kin, Contact details, Bank	HR Director
A5	LDCC Management Information	Reports, Plans, Strategies	Operations Manager
A6	LDCC Internal Information	Reports, Plans, Strategies	Operations Manager
A7	LDCC IT Systems	All files and data are in the system	IT Manager
A8	Computers - Desk PC's	Thin Clients, no data	Floor Manger
A9	Phones - Mobile	Mix of smartphones	IT Manager
A10	Phones - Desk	IP Phones	IT Manager
A11	Paper Files - Finance	Signed contracts and reports	Operations Manager
A12	Paper Files - General	Repors and general	Operations Manager
A13	Staff - Admin	5 x Work in bus support	Operations Manager
A14	Staff - Phone Operatives	150 x On phones	Floor Manger
A15	Staff - Management	6 x Managers and directors	CEO
A16	Staff - Temps	~ 10 - Used for high load shifts	HR Director
A17	IT - Main Server	IBM	IT Manager

	Information Asset	Details	Risk Owner
	GENERIC ASSETS		
	INTERNAL ISSUES		
II - 1	System age	See Security Context doc	IT Manager
II - 2	Sales driven history	See Security Context doc	CEO
II - 3	High staff turnover	See Security Context doc	HR Director
II - 4	Skills retention	See Security Context doc	HR Director
II - 5	Knowledge documentation	See Security Context doc	HR Director
II - 6	Information Availability	See Security Context doc	
II - 7	Processes undocumented	See Security Context doc	Operations Manager
II - 8	Contract security	See Security Context doc	Finance Director
II - 9	ISO 27002 adoption	See Security Context doc	CEO
II - 10	Sales enquiry levels	See Security Context doc	Sales Director
II - 11	Human Resource Security	See Security Context doc	HR Director
	EXTERNAL ISSUES		
EI - 1	Personal data market	See Security Context doc	CEO
EI - 2	Hacking and unauthorized interception	See Security Context doc	IT Manager
EI - 3	Wages	See Security Context doc	CEO
EI - 4	Power and connectivity	See Security Context doc	Operations Manager
EI - 5	Technology Expectations	See Security Context doc	IT Manager
EI - 6	Physical location	See Security Context doc	Facilities
EI - 7	Environmental	See Security Context doc	Facilities
EI - 8	`Employees taking LDCC or customer information to a competitor.	See Security Context doc	HR Director
EI - 9	Competitors solicitation	See Security Context doc	HR Director
	LEGAL		

	Information Asset	Details	Risk Owner
	GENERIC ASSETS		
L-1	Contract law	See Security Context doc	Finance Director
L-2	Health & Safety Legislation	See Security Context doc	Finance Director
	INTERESTED PARTIES		
IP - 1	Partners	See Security Context doc	CEO
IP - 2	Suppliers	See Security Context doc	Operations Manager
IP - 3	Insurers	See Security Context doc	Facilities
IP - 4	Government agencies	See Security Context doc	CEO
IP - 5	Management/Shareholders	See Security Context doc	CEO
IP - 6	Media / Commentators	See Security Context doc	Sales Director
IP - 7	Regulators	See Security Context doc	
IP - 8	Law enforcement	See Security Context doc	Facilities

Risk Assessment Template for ISO 27001 - D13 - Issue 1

	Risk Assessments	VERSION 1 - 9/01/20XX		Risk Assessment Date: 15/01/20xx	
Key	C - Confidentiality	1 - Lowest risk			
	I - Integrity	2 - Medium risk			
	A - Availability	**3 - Highest risk**			
	A V - Asset Value			(Imp = Implemented)	
	CHSQ - Consequences			(Ni = Not Implemented)	
	LKLH -Likelihood				

Asset Number	Asset Name	C	I	A	A V	CNSQ	Existing Controls	LKLH	Levelof Risk	Risk Treatment	Additional Controls	New Levels of Risk	Risk Owner Approval
	GENERIC ASSETS										Please see 'SOA' document		
A1	Customer provided information	2	3	2	7	3	Please see 'Controls' document	3	**63**	Reduce Likelihood	Imp	42	
A2	LDCC Customer contact Information	2	3	2	7	3	'	3	**63**	Accept	Ni	**63**	Sales Director
A3	LDCC Financial account information	3	3	3	9	3	'	2	54	Reduce Likelihood	Imp	27	Finance Director

Asset Number	Asset Name	C	I	A	A V	CNSQ	Existing Controls	LKLH	Levelof Risk	Risk Treatment	Additional Controls	New Levels of Risk	Risk Owner Approval
A4	LDCC HR Information	3	2	1	6	3	'	2	36	Accept	Ni	36	HR Director
A5	LDCC Management Information	1	1	1	3	3	'	1	9	Reduce	Imp	3	Operations Manager
A6	LDCC Internal Information	1	1	1	3	1	'	1	3	Reduce	Ni	3	Operations Manager
A7	LDCC IT Systems	3	3	3	9	3	'	3	81	Remove Source	Imp	81	IT Manager
A8	Computers - Desk PC's	2	1	1	4	2	'	3	24	Reduce Likelihood	Ni	24	Floor Manager
A9	Phones - Mobile	2	1	1	4	1	'	3	12	Change Consequences	Ni	12	IT Manager
A10	Phones - Desk	1	1	1	3	1	'	1	3	Share	Ni	3	IT Manager
A11	Paper Files - Finance	3	1	1	5	2	'	1	10	Remove Source	Ni	10	Operations Manager
A12	Paper Files - General	2	1	1	4	1	'	1	4	Change Consequences	Ni	4	Operations Manager
A13	Staff - Admin	2	1	1	4	2	'	3	24	Avoid	Ni	24	Operations Manager
A14	Staff - Phone Operatives	3	2	1	6	2	'	3	36	Avoid	Ni	36	Floor Manager
A15	Staff - Management	3	2	2	7	3	'	2	42	Share	Imp	28	IS Manager
A16	Staff - Temps	3	2	1	6	2	'	3	36	Share	Ni	36	HR Director

Asset Number	Asset Name	C	I	A	A V	CNSQ	Existing Controls	LKLH	Levelof Risk	Risk Treatment	Additional Controls	New Levels of Risk	Risk Owner Approval
A17	IT - Main Server	1	2	3	6	3	'	2	36	Change Consequences	Imp	22	IT Manager
A18	IT - Main Switches	1	1	3	5	2	'	2	20	Reduce Likelihood	Ni	20	
	INTERNAL ISSUES (See Context Doc)												
II - 1	System age	1	2	3	6	3	'	2	36	Accept	Ni	36	IT Manager
II - 2	Sales driven history	3	1	1	5	2	'	2	20	Reduce	Ni	20	IS Manager
II - 3	High staff turnover	2	2	1	5	2	'	2	20	Reduce	Ni	20	HR Director
II - 4	Skills retention	1	1	3	5	1	'	2	10	Change Consequences	Ni	10	HR Director
II - 5	Knowledge documentation	1	1	2	4	1	'	2	8	Reduce Likelihood	Ni	8	HR Director
II - 6	Information Availability	1	1	2	4	2	'	3	24	Reduce Likelihood	Ni	24	
II - 7	Processes undocumented	1	2	2	5	1	'	3	15	Reduce	Ni	15	Operations Manager
II - 8	Contract security	1	1	1	3	2	'	3	18	Reduce	Ni	18	Finance Director
II - 9	ISO 27002 adoption	2	2	2	6	2	'	3	36	Accept	Ni	36	IS Manager
II - 10	Sales enquiry levels	2	3	1	6	2	'	2	24	Reduce Likelihood	Ni	24	Sales Director
II -11	Human Resource Security	3	2	2	7	3	'	3	63	Reduce Likelihood	Imp	42	HR Director

Asset Number	Asset Name	C	I	A	A V	CNSQ	Existing Controls	LKLH	Levelof Risk	Risk Treatment	Additional Controls	New Levels of Risk	Risk Owner Approval
	EXTERNAL ISSUES (See Context Doc)												
EI - 1	Personal data market	3	1	1	5	3	'	3	**45**	Reduce Likelihood	Imp	30	IS Manager
EI - 2	Hacking and unauthorized interception	3	3	2	8	3	'	2	48	Accept	Ni	48	IT Manager
EI - 3	Wages	2	2	1	5	2	'	3	30	Reduce Likelihood	Ni	30	IS Manager
EI - 4	Power and connectivity	1	1	2	4	3	'	3	36	Accept	Ni	36	Operations Manager
EI - 5	Technology Expectations	1	1	2	4	2	'	3	24	Change Consequences	Ni	24	IT Manager
EI - 6	Physical location	3	2	3	8	2	'	3	**48**	Accept	Ni	32	Facilities
EI - 7	Environmental	1	1	2	4	3	'	3	36	Accept	Ni	36	Facilities
EI - 8	`Employees taking LDCC or customer information to a competitor.	2	1	1	4	2	'	2	16	Avoid	Ni	16	HR Director
EI - 9	Competitors solicitation	2	1	1	4	2	'	3	24	Accept	Ni	24	HR Director
	LEGAL (See Context Doc)												
L-1	Contract law	1	1	1	3	2	'	3	18	Accept	Ni	18	IS Manager
L-2	Health & Safety Legislation	1	1	1	3	3	'	3	27	Reduce Likelihood	Ni	27	Operations Manager

Asset Number	Asset Name	C	I	A	A V	CNSQ	Existing Controls	LKLH	Levelof Risk	Risk Treatment	Additional Controls	New Levels of Risk	Risk Owner Approval
	INTERESTED PARTIES (See Context Doc)												
IP - 1	Partners	3	2	2	7	2	'	3	42	Reduce Likelihood	Imp	28	IS Manager
IP - 2	Suppliers	2	3	1	6	1	'	3	18	Reduce	Ni	18	Sales Director
IP - 3	Insurers	3	1	1	5	2	'	3	30	Reduce	Ni	30	Facilities
IP - 4	Government agencies	3	2	1	6	2	'	3	36	Accept	Ni	36	Facilities
IP - 5	Management/Shareholders	3	1	1	5	3	'	3	45	Change Consequences	Imp	24	IS Manager
IP - 6	Media / Commentators	3	2	1	6	2	'	3	36	Accept	Ni	36	Sales Director
IP - 7	Regulators	3	1	1	5	2	'	3	30	Accept	Ni	30	
IP - 8	Law enforcement	3	1	1	5	3	'	3	45	Reduce Likelihood	Imp	30	Facilities

Asset Number	Asset Name	Statement of Applicability - D14 - Issue 1		
	GENERIC ASSETS	**Controls**	**Justification for Inclusion**	**Implemented? RTP Ref**
A1	Customer provided information	1. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. 2. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. 3. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Because customers send information to us in different ways we need it secured and safe. Policies make our staff follow accepted ways of doing things.	PartIal, RTP A1
A2	LDCC Customer contact Information	1. Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. 2. Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled. 3. Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Our customers information needs to remain accurate and complete, identifying ownership of sales documents helps prevent unauthorised editing. In the past sales staff have provided incorrect and incomplete information that has then been added to our CRM system. When we have updated systems in the past, records have been altered, we need to manage changes. In the past we have had malware infections that has damaged our data.	No
A3	LDCC Financial account information	1. Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. 2. Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents. 3. Physical security for offices, rooms and facilities shall be designed and applied.	Our financial information is sensitive so needs classifying. Incidents need managing quickly and efficiently. Rooms in finance should be locked.	Yes, RTP A3

A4	LDCC HR Information	1. Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. 2. Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents. Physical security for offices, rooms and facilities shall be designed and applied.	HR information is very sensitive so needs identifying as sensitive and protecting. HR office should be locked at all times.	No
A5	LDCC Management Information	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization. Physical security for offices, rooms and facilities shall be designed and applied. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.		Yes, RTP A5
A6	LDCC Internal Information	1. Physical security for offices, rooms and facilities shall be designed and applied. 2. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Our internal information should be locked away whenever possible as it can be accessed by many staff, non disclosure agreements are valuable.	No, RTP A6
A7	LDCC IT Systems	1. Equipment shall be correctly maintained to ensure its continued availability and integrity. 2. Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. 3. Rules governing the installation of software by users shall be established and implemented.	IT should be maintaining the equipment properly. It should be located in a good place and software not installed without asking..	No
A8	Computers - Desk PC's	1. Media shall be disposed of securely when no longer required, using formal procedures. 2. Rules governing the installation of software by users shall be established and implemented. 3. Rules for the development of software and systems shall be established and applied to developments within the organization.	If users use DC's or USB sticks to manipulate information, these should be deleted or destroyed after use. Users should not fiddle with programs because they could break it.	No

A9	Phones - Mobile	1. Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises. 2. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Mobiles contain a lot of information, often emails and so should be looked after. If used out of the office care should be taken using insecure public networks.	No
A10	Phones - Desk	1. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.2. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	New threats come along all the time. Out phones are network devices and we need support keeping them secure. If the power failed it can cause problems when the system restarts.	No
A11	Paper Files - Finance	1. Physical security for offices, rooms and facilities shall be designed and applied. 2. Procedures for working in secure areas shall be designed and applied.	Paper is easily seen and stolen. Locking rooms will protect the information. If we do have secure rooms, how they are used is important in keeping up security.	No
A12	Paper Files - General	1. Physical security for offices, rooms and facilities shall be designed and applied. 2. Procedures for working in secure areas shall be designed and applied. 3. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Paper is easily seen and stolen. Locking rooms will protect the information. If we do have secure rooms, how they are used is important in keeping up security. The clear desk policy helps with paper records.	No
A13	Staff - Admin	1. A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. 2. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Not all staff need to see all files and information. A formal structure helps protect information. When we send information to partners and suppliers we need to do it right and safely.	No

A14	Staff - Phone Operatives	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.		No
A15	Staff - Management	1. Media shall be disposed of securely when no longer required, using formal procedures. 2. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Our managers use a lot of information, often saved on mobile devices and media we need them to look after these items. They also work from their cars and homes so use insecure public connections sometimes.	Yes, RTP A15
A16	Staff - Temps	1. A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. 2. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Temps should only get the information they actually need - no more. As they may not know how to send information (our way) they will need more structure and guidance.	No
A17	IT - Main Server	1. Media shall be disposed of securely when no longer required, using formal procedures. 2. Procedures for working in secure areas shall be designed and applied. 3. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. Backups should be taken.	If the server is backed up the the media files used be securely wiped or destroyed after use. The server should be kept in a secure room and protected from power loss. Backups of systems are very important.	Yes, RTP A17
	INTERNAL ISSUES			
II - 1	System age	1. Equipment shall be correctly maintained to ensure its continued availability and integrity. 2. Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Older equipment needs to be maintained well. If we did have a failure backups would be needed.	No

II - 2	Sales driven history	1. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. 2. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities. 3. There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Sales staff are on the road and often take copies of customer files, these copies need to be controlled. We should define formal arrangements for how we should transfer files.	No
II - 3	High staff turnover	1. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced. 2. Operating procedures shall be documented and made available to all users who need them. 3. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	If staff leave often we need to be careful with how they are exited. As roles change, the definition of these roles must be clear and available. As ne staff will be unfamiliar with legislation, we should carefully set it out	No
II - 4	Skills retention	1. A policy on the use of cryptographic controls for protection of information shall be developed and implemented. 2. Operating procedures shall be documented and made available to all users who need them.	If we lost key skills such as how to encrypt or unencrypt files we would loose the information. We need to document all such procedures.	No
II - 5	Knowledge documentation	1. A policy on the use of cryptographic controls for protection of information shall be developed and implemented. 2. Operating procedures shall be documented and made available to all users who need them.	If we lost key skills such as how to encrypt or unencrypt files we would loose the information. We need to document all such procedures.	No
II - 6	Information Availability	1. Equipment shall be correctly maintained to ensure its continued availability and integrity. 2. Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. 3. Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	If equipment is not maintained it could fail and affect availability. Backups would also be needed. Redundant systems are important.	No

II - 7	Processes undocumented	1. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. 2. An access control policy shall be established, documented and reviewed based on business and information security requirements. 3. All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Processes can be helped if they are documented. Access control documents are often needed as reference. Our legal position could be affected if processes are undocumented.	No
II - 8	Contract security	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.		No
II - 9	ISO 27002 adoption	1. A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. 2. The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Policies would show staff the benefits of a structured ISO 27001 program. Reviewing the policies encourages management involvement and will help our argument.	No
II - 10	Sales enquiry levels	1. The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. 2. Information involved in electronic messaging shall be appropriately protected.	If we look out for issues like capacity we will be able to spot problems early.	No
II - 11	Human Resource Security	1. Background verification checks on all candidates for employment. 2. All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training. 3. There shall be a formal and communicated disciplinary process in place	It is important because our staff are the core of our organisation. They must be trustworthy and well disciplined, so as not to divulge information to outside parties.	Yes, RTP II11
	EXTERNAL ISSUES			

EI - 1	Personal data market	1. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. 2. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	We know our information has a value, Media used in the office should be protected just in case it is picked up. If staff leave they must not be allowed to sell our information.	Partial, EI1
EI - 2	Hacking and unauthorized interception	1. Password management systems shall be interactive and shall ensure quality passwords.2. The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Good passwords can help making hacking harder. Some programs can bypass passwords and compromise security, these should be controlled.	No
	LEGAL			
L-1	Contract law	1. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. 2. The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Loss of power can cause computers big problems, we could over load our systems and cause a failure.	No
L-2	Technology Expectations	No controls identified in ISO 27002		No
	INTERESTED PARTIES			
IP - 1	Environmental	1. The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. 2. The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	We know flooding and storms affects us, BC should be in place to protect us.	Partial, RTP IP1

IP - 2	`Employees taking LDCC or customer information to a competitor.	1. Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.	Sales staff work out of the office and could take data to a competitor.	No
IP - 3	Competitors solicitation	1. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. 2. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	We know information has a value, Media used in the office should be protected just in case it is picked up. If staff leave they must not be allowed to sell our information.	No
IP - 4	LEGAL	1. All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. 2. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Legal issues should always be treated seriously. Procedures would help us do the right thing.	No
IP - 5	Contract law	1. Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets shall be agreed with the supplier and documented. 2. All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. 3. Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	Contracts can be very complicated we need to make sure we do everything right. Different laws apply, we need to be sure which ones are important.	Yes, RTP IP5

IP - 6	Health & Safety Legislation	1. Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. 2. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. 3. The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	If an incident did occur, we need to respond well and safeguard out staff. Entrances where goods are being moved about are dangerous places.	No
IP - 7	INTERESTED PARTIES	1. Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. 2. Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Suppliers can take our information if we don't look after it. Managers should review their departmental suppliers.	No
IP - 8	Partners	1. Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. 2. Information security shall be addressed in project management, regardless of the type of the project.	Managers should review their departmental suppliers. Projects should always contain IS requirements.	Yes, RTP IP8

Information Security Risk Treatment Plan - RTP A -17

FOR: A – 17 ‘Backup (IT Main Server)’

22/04/20xx

D15 – Issue 1

Risk Treatment Plan Criteria

Developing a Risk Treatment Plan

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented.

Risk to be treated, reasoning and accountability

Risk

There are risks associated with the information security backup control relating to the protection against loss of data. These include server failure, power failure, and corruption of sensitive information which may give rise to loss, deletion or unavailability of information, software or system images.

Reasoning

Our information requires protecting, in order to ensure we can correct, secure and recover operations of our information processing. Information backup and testing ensures that the correct information is available and retrievable when and where required.

Accountability

John Bishop IT Manager is responsible for the approval of this plan. Colin Strange, IT Analyst, is responsible for plan implementation.

Proposed actions, resources and performance measures

Proposed Actions

Information should be protected by appropriate backup controls this will include:

1. Identify data to be backed up and required frequency
2. Identify media to be used and it’s handling requirements
3. Assign responsibility for completing backups
4. Establishing standard operating procedures for backup
5. Start to check the effectiveness of back up activities (‘Restoration’ testing)
6. Implement procedures and backups

Resources

1. John Bishop IT Manager shall be responsible for implementation of information backup processes and procedures
2. IT staff will be assigned to undertake the activities
3. Management will be responsible for the identification and request of specific backup requirements
4. Third party IT providers will be made available if required to provide support

Performance measures

1. Adherence to the implementation schedule
2. Verification records of backups are documented and retained (according to criteria)
3. ‘Restoration’ testing is carried out according to procedures
4. Testing of ‘Restoration’: data is then available, with no loss of integrity

Reporting, monitoring requirements and schedule

Reporting

The IS Manager will provide the next quarterly management meeting with a backup schedule report.

Monitoring

Internal audit will be invited to review the 3 performance measures.

Schedule

1. 2 Weeks
2. 2 Weeks after 1
3. 1 Week after 2
4. 2 months after 3
5. 1 Month after 4
6. Upon completion of 5

Information Security Risk Treatment Plan – RTP A1

FOR: ‘A1 Customer provided information’

18/08/20xx

D15 – Issue 1

Information Security Risk Treatment Plan

Developing a Risk Treatment Plan

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented.

Risk to be treated, reasoning and accountability

Risk
There is a risk to ‘Customer provided information’

Reasoning

Because customers send information to us in lots of different ways, we need it secured and safe while in transit and upon receipt. Malware could get into our systems through this route so we need to protect ourselves.

Accountability

Mr Swan, CEO is responsible for the approval of this plan. John Bishop, IT team leader is responsible for plan implementation.

Proposed actions, resources and performance measures

Proposed Actions

[Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.]

1. Formal exchange agreements shall be created to protect the transfer of information through the use of all types of communication facilities.
2. Formal exchange agreements shall be then implemented.
3. An appropriate policy & procedure shall be created to ensure exchange agreements are implemented.

Resources

5. Admin staff will be scheduled to undertake the exchange agreement activities on their normal prioritized rota.
6. A sum of £3,000 has been approved for the project. This has come from the IT server fund. Project Finance code: ASE 1234
7. If required external resource for our Legal supplier may be made available, this would require further authorization.

Performance measures

5. Formal transfer agreements in place.   Starting figure: 0%   Target: 90%

Constraints in achieving these targets include other urgent IT tasks such as responding to high sales activity and high staff turnover in IT.

Reporting, monitoring requirements and schedule

Reporting

IT will provide the next quarterly management meeting with an update report.

Monitoring

Internal audit will be invited to review incoming media from customers to verify it is protected in an acceptable way.

Schedule for proposed actions

1. 3 weeks
2. 3 months after 1
3. 2 months for policy & procedures

Information Security Risk Treatment Plan – RTP EI - 6

FOR: ‘EI – 6 Physical location (Physical entry controls)

02/07/20xx

D15 – Issue 1

Risk Treatment Plan Criteria

Developing a Risk Treatment Plan

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented.

Risk to be treated, reasoning and accountability

Risk

There are multiple risks associated with physical entry controls relating to protecting secure areas. These include access to areas containing sensitive information which may give rise to theft, fraud, information leakage, misuse or wilful damage to information or assets.

Reasoning

Our assets require managing, in order to prevent unauthorised physical access, damage and interference to the organisations information and information processing facilities. Sensitive areas of our facilities should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Appropriate entry controls for other offices, rooms and facilities should also be designed and implemented, commensurate to the identified risks and the value of the assets at risk in each setting.

Accountability

Simon Lock, Facilities Manager is responsible for the approval of this plan. Geoff King, Maintenance Engineer is responsible for plan implementation.

Proposed actions, resources and performance measures

Proposed Actions

Sensitive areas of information processing facilities should be protected by appropriate entry controls this will include:

7. Identify potential access locations where improved security could be implemented
8. Identify appropriate access requirement groups suitable for LDCC
9. Install locks and Key code or swipe card biometric authentication mechanism for all entry points (e.g. key card and/or PIN) as required
10. Provision of identification cards for visitors, temps and staff
11. Create appropriate ‘Physical Entry Control’ procedures

Resources

8. The Maintenance Engineer shall be responsible for implementation of physical entry processes and procedures
9. Facilities staff will be assigned to undertake the activities
10. Management will be responsible for the identification and request of specific screening requirements

Performance measures

1. Adherence to the implementation schedule
2. Completion of locks and access system installation
3. Audit of adherence to ‘card issuing’ procedures (new starter card issuing requests being actioned and leavers being de-activated)
4. Observation on the use of the system at peak entry times.

Reporting

Facilities will provide the next quarterly management meeting with an update report.

Monitoring

Internal audit will be invited to review the 3 performance measures.

Schedule

1. 2 Weeks

2. 2 Weeks after 1

3. 3 months after 2

4. With 3

5. With 3

Information Security Risk Treatment Plan – RTP II -11

FOR: ‘II – 11 Human Resources Security (Screening Control)’

22/05/20xx

D15 – Issue 1

Risk Treatment Plan Criteria

Developing a Risk Treatment Plan

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented.

Risk to be treated, reasoning and accountability

Risk

There are multiple risks associated to human resources relating to eligibility and suitability of employees. These include legal eligibility for employment, experience, competency and personal motivation which may give rise to poor performance, theft, fraud, information leakage, misuse or wilful damage to information or assets.

Reasoning

Our own assets need looking after, in order to reduce the likelihood of human resource related information security breaches, pre-employment screening ensures that unsuitable candidates are eliminated from the recruitment process.

Accountability

Raj Patel HR Director, is responsible for the approval of this plan. Sarah Pippins, Human Resources Manager is responsible for plan implementation.

Proposed actions, resources and performance measures

Proposed Actions

1. Create and communicate the screening policy, to include the implementation of the following screening checks:
   - Name
   - Address
   - Nationality (passport or proof of naturalisation)
   - Marital status
   - Education and qualifications
   - Previous Employment
   - Criminal record declaration and spent convictions
   - Two references (including at least one previous employer)

2. Procedures for carrying out pre-employment screening shall be developed and implemented
3. Procedures shall be developed to identify and undertake specific screening requirements for privileged roles or as specifically required for a customer

Resources

11. The Human Resources Manager shall be responsible for implementation of screening processes and procedures
12. Human Resources staff will be assigned to undertake the activities
13. Management will be responsible for the identification and request of specific screening requirements

Performance measures

6. Procedures for pre-employment screening shall be developed and implemented in accordance with the below schedule
7. Screening for all new employees to start no later than three months from the commencement of this Treatment Plan
8. Completed HR records for screened employees to be available for inspection upon commencement of screening

Reporting, monitoring requirements and schedule

Reporting

HR will provide the next quarterly management meeting with an update report.

Monitoring

Internal audit will be invited to review the 3 performance measures.

Schedule

4.	1 month
5.	1 month after 1
6.	1 month after 2

Objectives, Resource and Competence

IS Objectives and plans – OBJ A2

FOR: ‘OBJ A2 LDCC Customer contact Information’

22/03/20xx

D16 – Issue 2

Customer Contact Details

Developing an IS Objectives plan

The purpose of an' IS Objectives plan' is to set out how an intended action will be achieved, who will undertake it and how it will be measured.

Objectives to be achieved

Issues to be addressed

'Asset A2 LDCC Customer contact Information' – This is information about LDCC's customers. This information needs to remain accurate and complete. In the past sales staff have provided incorrect and incomplete information that has then been added to our CRM system. The main locations identified as containing this information are:

1. The CRM system
2. Sales staff's computers
3. Written notes from meetings

Proposed Actions

4. Procedures for validating 'LDCC Customer contact Information' prior to loading into the CRM system will be developed
5. All Sales staff will undergo training on our requirements.

Accountability

Clive Page, Acting Sales Director is responsible for the approval of this plan. Debbie Cockram from Operations is responsible for plan implementation.

Resources and responsibilities

14. Sales will provide staff (unspecified at this stage) to develop procedures for validating 'LDCC Customer contact Information' prior to loading into the CRM system.
15. Debbie Cockram from Operations will probably deliver the training.

Completion schedule

1. 1 month after permanent sales director appointed
2. As and when this is needed

Evaluating results

1. Internal audit will review 'new' data loaded on to the CRM system for errors to assess if the 'Procedures for handling LDCC Customer contact Information' is being followed.

2. All sales staff to attend training

IS Objectives and Plans – OBJ EI - 2

FOR: ‘OBJ EI - 2 Hacking and Unauthorised Interception’

01/01/20xx

D16 – Issue 2

Hacking and Unauthorised Interception

Developing an IS Objectives plan

The purpose of an' IS Objectives plan' is to set out how an intended action will be achieved, who will undertake it and how it will be measured.

Objectives to be achieved

Issues to be addressed

Our current firewalls are old and are insufficient to prevent new threats. 'Hacking and Unauthorised Interception' – This is the deliberate interception or collection of data or voice traffic on our network. Competitors or thieves seek to gather personal information that enables them to commit fraud. Although we have not detected this happening as yet, it is a real and present concern. The main ways this is done are:

4. External parties gaining access to our IT systems
5. Staff finding ways to access restricted information internally

Proposed Actions

Replace our existing external firewalls with Enterprise grade products that offer state-full inspection capabilities. The design must contain the most advanced firewall capabilities, including:

- proxies (including SOCKS)
- stateful inspection or dynamic packet filtering
- network address translation
- virtual private networks
- Internet Protocol version 6 or other non-Internet Protocol version 4 protocols
- network and host intrusion detection technologies

External Firewall deployment steps

Prepare	1. Ensure network diagrams are up to date
Configure	2. Select and acquire firewall hardware and software as above
	3. Acquire firewall documentation, training, and support
	4. Install firewall hardware and software
	5. Configure IP routing
	6. Configure firewall packet filtering
	7. Configure firewall logging and alert mechanisms
Test	8. Test the firewall system

Deploy 9. Install the firewall system

10. Phase the firewall system into operation

Internal Intellectual Property control deployment steps

Implement internal Intellectual Property Controls based on information signatures.

Prepare 11. Information signatures identification – credit card details, personal information.

12. Assign approved locations for information types

13. Approve staff access structure

14. Select and acquire agents and management application

Configure 15. Implement tracking agents onto PC's and servers

16. Acquire firewall documentation, training, and support

17. Configure physical server

18. Configure logging and alert mechanisms

Test 19. Test the system

Deploy 20. Enable the live the IP system

Accountability

John Bishop IT Manager is responsible for the approval of this plan. Chris Flood, IT **Analyst** is responsible for plan implementation.

Resources and responsibilities

Resources and responsibilities

16. Management will provide budget (to be set) for the purchase of new Firewalls, budget is still pending. Objective is on hold.
17. IT will project manage the process but a specialist supplier will undertake this work.

Completion schedule

1. Implementation Resource Estimates

The following rough-order-magnitude timeframes represent the calendar time required by staff / supplier to implement each of the practices described in the 'Proposed Actions section'.

1. Design the firewall system 3 months
2. Acquire firewall hardware and software 2 months

3. Acquire firewall documentation, training, and support 1 month

4. Install firewall hardware and software 1 month

5. Configure IP routing 1 week

6. Configure firewall packet filtering 3 weeks

7. Configure firewall logging and alert mechanisms 2 weeks

8. Test the firewall system 2 weeks

9. Install the firewall system 1 week

10. Phase the firewall/IP system into operation 2-3 months

Evaluating results

1. Internal and external penetration testing (undertaken by a third party) will be undertaken to ensure successful deployment.

IS Objectives and Plans – OBJ EI - 5

FOR: ‘OBJ EI - 5 Technology Expectations’

08/09/20xx

D16 – Issue 2

Technology Expectations

Developing an IS Objectives plan

The purpose of an' IS Objectives plan' is to set out how an intended action will be achieved, who will undertake it and how it will be measured.

Objectives to be achieved

Issues to be addressed

A new and important customer has stipulated that all traffic between ourselves and the customer be encrypted using SSL or better encryption. In the past we have not done this so new procedures and potentially equipment will be needed. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that are designed to provide communication security over the Internet. Several versions of the protocols are in wide spread use to protect data in web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

Proposed Actions

1. Decide with the customer the encryption requirement
2. Identify what data is to be encrypted
3. Write procedures to include (our) sent and their (receive) IP addresses.
4. Undertake live testing with the customer
5. Deploy service

Accountability

John Bishop IT Manager is responsible for the approval of this plan. Chris Flood, IT **Analyst** is responsible for plan implementation. Mr Swan CEO will instigate the plan.

Resources and responsibilities

Resources and responsibilities

18. Management will advise on the likelihood of the customer purchasing our services and issue a ‘GO’ instruction.
19. Managing director to provide the financial budget for the IT equipment
20. IT to provide staffing resource and budget estimate for approval.

Completion schedule

1. 1 month

2. 2 weeks after 1

3. 1 month after 2
4. 1 month after 3
4. After 4

Evaluating results

1. LDCC staff will review (with the customer) successful document transfers and failed transfers.

Review

1st Review – 8/10/20xx (carried out by Chris Flood with IT manager)

Proposed action 1 has now been completed with the customer and the encryption selected is SSL.

2nd Review – 10/11/20xx (carried out by Chris Flood with IT manager)

Proposed action 2 has now been completed, data to be encrypted is electronic mail and Internet faxing only.

2rd Review – Scheduled for 10/12/20xx to be carried out by Chris Flood with IT manager in attendance

Resources [Determined to be necessary] & Provision Records (Extract) – D17 – Issue 2

#	Infrastructure Determined	Rationale (Why?)	Provision Date/Comments
I1	Physical access controls – window locks, secure door locks & combination locks, card access system, key station, color magnetic card printer, cards blank Total £4,000	Need physical access controls for all staff and visitors etc.	22/09/xx Invoice 54321,
I2	IT Backups facilities – Servers, tapes, CD's etc.	Need to back up our critical servers	August 20xx
I3	Hacking & authorised interception equipment (see OBJ E1-2)	Need to prevent deliberate hacking from our staff and others into our servers	Budget is still pending – See Objective
I4	SSL Encryption or better (see OBJ EI-5)	Need to protect data from customer's during transfer	See Objective Reviews
I5	Building alarms, sensors, controls, video etc.	Need to raise an alarm to inform the Police of a break-into our premises	Need a new system – ours is currently very old and will not do the job. Budget to be set next year (hopefully)
I6	Premises that are adequately protected in a suitable low risk location (or high risk and control)	Need to protect our assets from outside attack	Current building is not in the best location for IS. Hence the controls in I1 above are critical
	Human Resource Determined	**Rationale (Why?)**	**Provision Date/Comments**
R1	Information Security Manager/ Management Representative for ISMS	Need the focus & skills and point of contact for IS skills	26/10/06 – Clive Pritchard

R2	IT Manager	Need the focus & skills and point of contact for IT skills -Network security	09/11/08 – John Bishop
R3	IT Backup up - human resource	Need to daily back up critical servers	18/01/11 – Graham Spring
R4	Physical Access Security – human resource	Need to maintain physical access security	17/05/09 – Simon Lock 15/12/05 – Geoff King
R5	Human screening resource	Need to screen new staff before starting	12/06/03 – Sarah Pippins 10/02/01 – Tracey Baker
R6	ISMS Auditors	Need to audit the ISMS	01/10/03 – Gordon Black 03/03/06 – Fay Woodward
R7	Management Review - Top Management	Need Top management to review the ISMS	06/04/97 – Alan Swan 12/07/99 – Joe Cullum 24/9/07 – Carly Hudd 22/7/05 – Peter Gaut 23/02/02 – Clive Page - Raj Patel
R8	Receptionist	Need to provide temporary cards & visitor cards	03/12/10 – Lauren Hunter
	Finance Determined	**Rationale (Why?)**	**Provision Date/Comments**
F1	£125,000 – Labor	Some jobs are not purely of an IS nature, so can reduce the total wage costs above	Provided, as detailed above
F2	£ 45,000/year over 5 years – Infrastructure	Can amortised fixed assets over 5 years + card replacement costs etc.	Provided, as detailed above

Staff List (Extract) – D18- Issue 4

Name	Department	Position	Joined	Left
Alan Swan	Executive	MD/CEO	06/04/97	
Joe Cullum	Executive	Chief Operation Officer	12/07/99	
Carly Hudd	Executive	Finance Director	24/9/07	
Peter Gaut	Executive	Resources Director	22/7/05	
Clive Page	Sales & Marketing	Sales Manager/Acting Sales Director	23/02/02	16/11/XX
Lucy Carr	Operations	Tele Manager	16/07/05	
Clive Prichard	IT	IS Manager/Management representative for ISMS	26/10/06	
Amanda French	Operations	Operations Manager	23/04/09	
Rodney Trotter	Finance	Finance Manager	23/02/09	
Philip Hernshaw Smyth	Finance	Accounts Manager	23/02/02	
Lauren Hunter	Facilities	Receptionist	03/12/10	01/11/XX
Kate Lough	Operations	Phone Operative	07/07/07	
Amanda Lomond	Operations	Phone Operative	03/10/13	
Graham Spring	IT	Analyst/Systems Admin	18/01/11	
Colin Strange	IT	Analyst	22/11/10	
Simon Lock	Facilities	Facilities Manager	17/05/09	
Geoff King	Facilities	Maintenance Engineer	15/12/05	
Chris Flood	IT	Analyst	17/03/04	
Raj Patel	HR	HR Director		
Sarah Pippins	HR	HR Manager	12/06/03	
Tracey Baker	HR	HR Assistant	10/02/01	
Gordon Black	Controls Assurance	Controls Manager/ISMS Auditor	01/10/03	
John Bishop	IT	Team Leader/IT Manager	09/11/08	
Teddy	Operations	Team Leader	10/04/10	15/10/XX

Name	Department	Position	Joined	Left
Armstrong				
Fay Woodward	Operations	Team Leader/ISMS Auditor	03/03/06	
Michael Hamilton	Operations	Phone Operative	17/09/10	
Ian Smith	Operations	Phone Operative	20/07/10	
Anthony Summer	Operations	Phone Operative	13/09/08	
Debbie Cockram	Operations	Phone Operative / Sales Assistant	10/03/09	
Nigel Fairford	Operations	Phone Operative	05/01/12	
Earl Hickey	Operations	Phone Operative	28/04/11	
Ron Childress	Operations	Phone Operative	12/05/11	
Evan Schmidt	Operations	Phone Operative	10/11/10	
Lauren Hunter	Operations	Phone Operative	08/05/12	25/01/XX
Nicky Lacey	Operations	Phone Operative	13/08/13	
Nathalie Romford	Operations	Phone Operative	05/02/13	
Derek Boduke	Operations	Phone Operative	17/05/13	
Yan Kypers	Operations	Phone Operative	02/09/12	
Joss Taylor	Operations	Phone Operative	06/11/12	
Melanie Hope	Operations	Phone Operative	19/08/10	
Suzanne Thatcher	Operations	Phone Operative	13/05/11	
Alex Thornton	Operations	Phone Operative	03/09/07	12/03/XX
Dan Hasham	Operations	Phone Operative	26/03/08	
Reggie Gates	Operations	Phone Operative	12/06/11	
Jodie Brady	Operations	Phone Operative	06/07/13	
Tom Bilsdon	Operations	Phone Operative	16/10/12	
Dean Francis	Operations	Phone Operative	29/05/10	
James Franchitti	Operations	Phone Operative	17/06/09	
Sarah Wallmarsh	Facilities	Janitor/Cleaner	23/04/04	
Kayla Norman	Facilities	Janitor/Cleaner	05/06/07	10/07/XX

Name	Department	Position	Joined	Left
Wima Tenson	Facilities	Janitor/Cleaner	08/10/04	
Demi Taunton	Operations	Phone Operative	20/09/12	
Arnold Tintinhall	Operations	Phone Operative	10/05/11	05/10/XX
Graham Bell	Operations	Phone Operative	04/08/12	
Anne Parsons	Operations	Phone Operative	10/09/11	
Kevin Grey	Operations	Phone Operative	08/05/12	

Training [Determined to be necessary] Records (Extract) – D19 – Issue 3

Name	Position	IS/MS Awareness	ISMS Auditing	IS Risk Assessment	RTP's	ISMS Objectives	IS LAW	IS ISO 27002 Controls	IS Event Reporting
Alan Swan	MD/CEO	|			|	|	|		|
Peter Gaut	Resources Director	|			|	|			|
Clive Page	Sales Manager/ Acting Sales Director								
Clive Prichard	IS Manager/ Management representative for ISMS	|		|	|	|	|	|	|
Amanda French	Operations Manager	|			|			|	|
Philip Hernshaw Smyth	Accounts Manager	|							|
Lauren Hunter	Receptionist	|							|
Kate Lough	Phone Operative	|					|		|
Amanda Lomond	Phone Operative	|							|

Name	Position	IS/MS Awareness	ISMS Auditing	IS Risk Assessment	RTP’s	ISMS Objectives	IS LAW	IS ISO 27002 Controls	IS Event Reporting
Graham Spring	Analyst/System Admin	✓		✓	✓				✓
Colin Strange	Analyst	✓			✓				✓
Simon Lock	Facilities Manager	✓		✓			✓	✓	✓
Geoff King	Maintenance Engineer	✓			✓				✓
Chris Flood	Analyst	✓			✓	✓			✓
Raj Patel	HR Director	✓			✓		✓		
Sarah Pippins	HR Manager	✓		✓	✓		✓		✓
Tracey Baker	HR Assistant	✓							✓
Gordon Black	Controls Manager/ ISMS Auditor	✓	✓	✓	✓		✓	✓	✓
John Bishop	Team Leader/ IT Manager	✓		✓	✓	✓	✓	✓	✓
Fay Woodward	Team Leader/ ISMS Auditor	✓	✓	✓	✓		✓	✓	✓

Dated: 01/January/20xx-1

Signed: Tracy Baker (HR Assistant)

Training Record – Clive Prichard – D20 – Issue 1

Course	Competence Level (Scale 1 - 5)	Training Needs
IS/MS **Awareness**	5 – Fully competent	None
ISMS Auditing	N/A	None
IS Risk Assessment	1 – New starter on RA	Training on IS RA required urgently (by year end/xx)
RTP’s	5 – Fully competent	None
ISMS Objectives	5 – Fully competent	None
IS LAW	3 – Needs additional guidance	Training on IS Law required by 01/10/xx
IS ISO 27002 Controls	3 – Needs additional guidance	
IS Event Reporting	5 – Fully competent	None
IS Nonconformity/CA sign off	5 – Fully competent	None
Practitioner Certificate in IRM (PCIRM)		Try and complete by 01/10/xx

Dated: 01/January/20xx

Signed: Raj Patel (HR Director)

Training Record – Fay Woodward – D20 – Issue 1

Course	Competence Level (Scale 1 - 5)	Training Needs
IS/MS Awareness	1 – New starter on IS/MS	Missed her induction – scheduled for next available induction
ISMS Auditing	N/A	None
IS Risk Assessment	5 – Fully competent	None
RTP's	3 – Needs additional guidance	Not sure yet
ISMS Objectives	5 – Fully competent	None
IS LAW	N/A	None
IS ISO 27002 Controls	5 – Fully competent	None
IS Event Reporting	5 – Fully competent	None
Certificate in Information Security Management Principles (CISMP)	1 – New starter on IS/MS	NEEDED - by 01/05/xx

Dated: 01/January/20xx-1

Signed: Sarah Pippins (HR Manager)

Training Record –Kate Lough – D20- Issue 1

Course	Competence Level (Scale 1 - 5)	Training Needs
IS/MS **Awareness**	5 – Fully competent	None
ISMS **Auditing**	N/A	None
IS Risk **Assessment**	N/A	None
RTP's	N/A	None
ISMS Objectives	N/A	None
IS LAW	N/A but….	Has shown an interest
IS ISO 27002 Controls	N/A	None
IS Event Reporting	5 – Fully competent	None

Dated: 01/January/20xx

Signed: Tracy Baker (HR Assistant)

Operation and Monitoring

Compliance Policy – D21 - Issue 1

Policy for compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software

A. Laws, Regulations and Contractual Requirements

For every LDCC information system, all relevant statutory, regulatory, and contractual requirements must be thoroughly identified, explicitly defined, and taken into account in business processes. The focus of this policy will be those specifically relating to intellectual property rights and use of proprietary software

15. 1.2 Intellectual Property Rights

A. Software Development Source

Software that supports business applications must be either developed in-house, or obtained from a known and reliable third-party vendor. Free software (also known as shareware) is not permitted unless specifically evaluated and approved by the Information Security Forum.

B. Information owned by / provided by customers

LDCC use of information must only extend usage as agreed with the customer under contract.

C. Information Attribution

LDCC staff must always give proper credit to the source of information used for LDCC activities.

D. Intellectual Property Labelling

All users who submit information in reports must reference the ownership of the information and any security requirements.

E. Software Copyright Notices

All computer programs and program documentation owned by LDCC must include appropriate copyright notices.

F. Multiple Copies of Information

Unless permission from the copyright owner(s) is first obtained, making multiple copies of material from databases, lists and other publications is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

G. Contract and Agreement Reviews

The agreements for all date use from third parties must be periodically reviewed for LDCC compliance.

I. Authorised Copies of Software

Management must make appropriate arrangements with all information owners for copies, if and when additional copies are needed for business activities.

J. Making Copies of Data

Third-party data in the possession of LDCC must not be copied unless such copying is consistent with relevant license agreements and either management has previously approved of such copying, or copies are being made for contingency planning purposes.

K. Unauthorised Copyrighted Information

Third-party copyrighted information, that LDCC does not have specific approval to store and/or use, must not be stored on LDCC systems or networks. Systems Administrators will remove this information or software, unless authorisation from the rightful owner(s) can be provided by the involved users.

L. Default Copyright Protection

Much of the material on LDCC’s systems is copyrighted or otherwise protected by intellectual property law (for instance by license agreement). Staff must investigate intellectual property rights for all material they discover on the Internet before using it for any other purpose. One exception to this rule involves internal electronic mail.

M. Redistribution of Information Posted On-Line

Staff using LDCC computers and communication systems must not redistribute information (music, software, graphics, text, etc.) that they access via the Internet unless they have confirmed that such a re-distribution is expressly permitted by the copyright owner. Every expression, as manifested in digital content, must be assumed to be copyrighted unless a notice to the contrary is posted in the same location.

N. Software Duplication

Users must not copy software provided to or by LDCC to any storage media, transfer such software to another computer, or disclose such software to outside parties without written permission from Information Technology Department.

O. Unauthorised Software and Data Copies

LDCC strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet users or other system users make unauthorised copies of software, the users are doing so on their own behalf, since all such copying is strictly forbidden by LDCC. Likewise, LDCC allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

P. Unauthorised Copyrighted Material

Worker participation in any manner with pirated software bulletin boards or related Internet sites is strictly prohibited, even if this participation occurs during non-working hours. This prohibition extends to any other facility or system which exchanges illegal copies of music, books, or other copyrighted material over the Internet or through other communications channels.

Q. Copyrighted Electronic Books

All electronic books or other text-based copyrighted works published by LDCC on the Internet or on any other publicly-accessible networked system must be in bit-mapped form.

R. Use of Third-Party Trademarks

LDCC web and commerce sites must not use any other organisation’s trademarks or service marks anywhere unless the usage reflects the actual attributes of LDCC products or services, and advance permission has been obtained from the Company Secretary.

S. Third-Party Confidentiality Agreements

Staff must not sign confidentiality agreements provided by third parties without the advance authorisation of the Company Secretary.

Procedures for the above need to be created and incorporated into the ISMS, in progress…….. John Bishop IT Team Leader

Information Exchange Agreement – D22 - Issue 1

THIS NON-DISCLOSURE AND SENSITIVE INFORMATION EXCHANGE AGREEMENT (hereinafter the "Agreement") is effective upon execution by both Parties, by and between **Andromeda IT**, and Lake Dale Contact Centre, a company. Both entities are herein referred to as "**The Parties**".

NOW, THEREFORE, in consideration of these promises and agreements hereinafter contained, **The Parties**, for mutual consideration in the form of information to be exchanged, agree as follows:

1. "Sensitive Information" shall mean Information including customer details, personal information under the Data Protection Act (or covering legislation) trade secret information of any kind, including but not limited to trade secret information of a business, planning, marketing, or technical nature, disclosed to the Receiving Party in connection with this Agreement, whether disclosed in written or documentary form or orally or visually, or by models, tools, or other hardware. The Receiving Party shall hold in confidence and not disclose to any third party, nor to any employee (except on a "need to know" basis) all Sensitive Information disclosed to it by the Disclosing Party which is identified by the Disclosing Party at the time of disclosure as being Sensitive Information.

2. **The Parties** agree that all Sensitive Information hereunder disclosed shall be used only as is reasonably required to accomplish the purpose(s) outlined above. When disclosed in writing the information shall be identified and labelled as Sensitive Information. When disclosed orally, such information shall first be identified as Sensitive Information at the time of the oral disclosure with subsequent confirmation in writing within twenty (20) calendar days after disclosure referencing the data and specifically identifying the Sensitive Information which was orally disclosed. **The Parties** agree to clearly label as "SENSITIVE INFORMATION" all information reduced to writing by either party as a result of such oral disclosures, or otherwise disclosed in writing hereunder.

3. Information Transfer Media and Processes.

Information shall be transferred between the parties in the following manner and only in this manner.

Sensitive information - Secure network VPN or Encrypted media

Non Sensitive information – Email, network or media

4. The Receiving Party agrees to apply, to all Sensitive Information disclosed in accordance with the provisions of this Agreement, the same degree of care with which it treats and protects its own Sensitive information against public disclosure but in no event les than a reasonable degree of care. All such Sensitive Information shall not be disclosed without the prior written consent of the party whose data are to be disclosed. **The Parties** agree that all Sensitive Information disclosed hereunder shall remain the property of the Disclosing Party and that said Sensitive Information shall not be copied nor reproduced without the express written approval of the Disclosing party, except for such copies as may be reasonably required for internal evaluation purposes by those persons with the requisite "need to know". Upon written notice, all Sensitive Information shall be returned to the Disclosing Party within thirty (30) calendar days after termination of this Agreement or such

5. The Receiving Party agrees to restrict its use and dissemination of the Sensitive Information within its own organization on a strict "need to know" basis.

6. The term of this Agreement shall be twelve (12) calendar months from the effective date, unless otherwise terminated in accordance with the provisions hereof. The obligations hereto relating to the disposition and use of Sensitive Information shall survive the expiration or termination of this Agreement for a period of three (3) calendar years.

7. Neither party hereunder shall assign nor transfer any of its rights or obligations hereunder without the prior written consent of the other party.

8. This Agreement may be terminated by either party on thirty (30) calendar days written notice to the other, provided, however, that no such termination shall serve to release the Receiving Party from its obligations as to disposition and use of Sensitive Information previously disclosed hereunder, which obligations shall remain in force in accordance with these provisions.

9. In the event of termination, the Receiving Party agrees to return to the Disclosing Party all documents and copies of the Sensitive Information disclosed in accordance with this Agreement.

10. This Agreement constitutes the entire understanding of **The Parties** hereto related to the disclosure and protection of Sensitive Information and supersedes all prior or contemporaneous written or oral agreements or understandings.

11. This Agreement shall be construed in accordance with the laws of the State of Florida without regard to its conflict of law principles, and shall not be amended nor modified except by written instrument signed by both parties hereto.

IN WITNESS WHEREOF, **The Parties** hereto have caused this instrument to be executed in their names by their duly authorized and proper officials as designated below:

Andromeda IT		LDCC	
Person:	Susan Clifton	Person:	Lauren Hunter
Title:	Post room Supervisor	Title:	Reception
Address:	33 Something	Address:	The Town
	Apples		The City
	Picklebrough		
Phone:	0143565654	Phone:	012345677890
Date:	25.09.20xx	Date:	25.09.20xx

Information Exchange Agreement – D22 – Issue 1

THIS NON-DISCLOSURE AND SENSITIVE INFORMATION EXCHANGE AGREEMENT (hereinafter the “Agreement”) is effective upon execution by both Parties, by and between **Epsom CCS**, and Lake Dale Contact Centre, a company. Both entities are herein referred to as “**The Parties**”.

NOW, THEREFORE, in consideration of these promises and agreements hereinafter contained, **The Parties**, for mutual consideration in the form of information to be exchanged, agree as follows:

1. “Sensitive Information” shall mean Information including customer details, personal information under the Data Protection Act (or covering legislation) trade secret information of any kind, including but not limited to trade secret information of a business, planning, marketing, or technical nature, disclosed to the Receiving Party in connection with this Agreement, whether disclosed in written or documentary form or orally or visually, or by models, tools, or other hardware. The Receiving Party shall hold in confidence and not disclose to any third party, nor to any employee (except on a “need to know” basis) all Sensitive Information disclosed to it by the Disclosing Party which is identified by the Disclosing Party at the time of disclosure as being Sensitive Information.

2. **The Parties** agree that all Sensitive Information hereunder disclosed shall be used only as is reasonably required to accomplish the purpose(s) outlined above. When disclosed in writing the information shall be identified and labelled as Sensitive Information. When disclosed orally, such information shall first be identified as Sensitive Information at the time of the oral disclosure with subsequent confirmation in writing within twenty (20) calendar days after disclosure referencing the data and specifically identifying the Sensitive Information which was orally disclosed. **The Parties** agree to clearly label as “SENSITIVE INFORMATION” all information reduced to writing by either party as a result of such oral disclosures, or otherwise disclosed in writing hereunder.

3. Information Transfer Media and Processes.

Information shall be transferred between the parties in the following manner and only in this manner.

Sensitive information - Secure network VPN or Encrypted media

Non Sensitive information – Email, network or media

4. The Receiving Party agrees to apply, to all Sensitive Information disclosed in accordance with the provisions of this Agreement, the same degree of care with which it treats and protects its own Sensitive information against public disclosure but in no event less than a reasonable degree of care. All such Sensitive Information shall not be disclosed without the prior written consent of the party whose data are to be disclosed. **The Parties** agree that all Sensitive Information disclosed hereunder shall remain the property of the Disclosing Party and that said Sensitive Information shall not be copied nor reproduced without the express written approval of the Disclosing party, except for such copies as may be reasonably required for internal evaluation purposes by those persons with the requisite “need to know”. Upon written notice, all Sensitive Information shall be returned to the Disclosing Party within thirty (30) calendar days after termination of this Agreement or such

5. This Agreement may be terminated by either party on thirty (30) calendar days written notice to the other, provided, however, that no such termination shall serve to release the Receiving Party from its obligations as to disposition and use of Sensitive Information previously disclosed hereunder, which obligations shall remain in force in accordance with these provisions.

6. In the event of termination, the Receiving Party agrees to return to the Disclosing Party all documents and copies of the Sensitive Information disclosed in accordance with this Agreement.

7. This Agreement constitutes the entire understanding of **The Parties** hereto related to the disclosure and protection of Sensitive Information and supersedes all prior or contemporaneous written or oral agreements or understandings.

8. This Agreement shall be construed in accordance with the laws of the State of Florida without regard to its conflict of law principles, and shall not be amended nor modified except by written instrument signed by both parties hereto.

IN WITNESS WHEREOF, **The Parties** hereto have caused this instrument to be executed in their names by their duly authorized and proper officials as designated below:

Epsom CCS

Person: Amanda Street

Title: Sales Director

Address: 33 Something
Apples
Picklebrough

Phone: 0435456790

Date: 27.09.20xx

LDCC

Person: Mr Swan

Title: CEO

Address:
The Town
The City

Phone: 012345677890

Date: 27.09.20xx

Information Exchange Agreement – D22 – Issue 1

THIS NON-DISCLOSURE AND SENSITIVE INFORMATION EXCHANGE AGREEMENT (hereinafter the "Agreement") is effective upon execution by both Parties, by and between **_____**, and Lake Dale Contact Centre, a company. Both entities are herein referred to as "**The Parties**".

NOW, THEREFORE, in consideration of these promises and agreements hereinafter contained, **The Parties**, for mutual consideration in the form of information to be exchanged, agree as follows:

1. "Sensitive Information" shall mean Information including customer details, personal information under the Data Protection Act (or covering legislation) trade secret information of any kind, including but not limited to trade secret information of a business, planning, marketing, or technical nature, disclosed to the Receiving Party in connection with this Agreement, whether disclosed in written or documentary form or orally or visually, or by models, tools, or other hardware. The Receiving Party shall hold in confidence and not disclose to any third party, nor to any employee (except on a "need to know" basis) all Sensitive Information disclosed to it by the Disclosing Party which is identified by the Disclosing Party at the time of disclosure as being Sensitive Information.

2. **The Parties** agree that all Sensitive Information hereunder disclosed shall be used only as is reasonably required to accomplish the purpose(s) outlined above. When disclosed in writing the information shall be identified and labelled as Sensitive Information. When disclosed orally, such information shall first be identified as Sensitive Information at the time of the oral disclosure with subsequent confirmation in writing within twenty (20) calendar days after disclosure referencing the data and specifically identifying the Sensitive Information which was orally disclosed. **The Parties** agree to clearly label as "SENSITIVE INFORMATION" all information reduced to writing by either party as a result of such oral disclosures, or otherwise disclosed in writing hereunder.

3. Information Transfer Media and Processes.

Information shall be transferred between the parties in the following manner and only in this manner.

Sensitive information - Secure network VPN or Encrypted media

Non Sensitive information – Email, network or media

4. The Receiving Party agrees to apply, to all Sensitive Information disclosed in accordance with the provisions of this Agreement, the same degree of care with which it treats and protects its own Sensitive information against public disclosure but in no event les than a reasonable degree of care. All such Sensitive Information shall not be disclosed without the prior written consent of the party whose data are to be disclosed. **The Parties** agree that all Sensitive Information disclosed hereunder shall remain the property of the Disclosing Party and that said Sensitive Information shall not be copied nor reproduced without the express written approval of the Disclosing party, except for such copies as may be reasonably required for internal evaluation purposes by those persons with the requisite "need to know". Upon written notice, all Sensitive Information shall be returned to the Disclosing Party within thirty (30) calendar days after termination of this Agreement or such

5. The Receiving Party agrees to restrict its use and dissemination of the Sensitive Information within its own organization on a strict "need to know" basis.

6. The term of this Agreement shall be twelve (12) calendar months from the effective date, unless otherwise terminated in accordance with the provisions hereof. The obligations hereto relating to the disposition and use of Sensitive Information shall survive the expiration or termination of this Agreement for a period of three (3) calendar years.

7. Neither party hereunder shall assign nor transfer any of its rights or obligations hereunder without the prior written consent of the other party.

8. This Agreement may be terminated by either party on thirty (30) calendar days written notice to the other, provided, however, that no such termination shall serve to release the Receiving Party from its obligations as to disposition and use of Sensitive Information previously disclosed hereunder, which obligations shall remain in force in accordance with these provisions.

9. In the event of termination, the Receiving Party agrees to return to the Disclosing Party all documents and copies of the Sensitive Information disclosed in accordance with this Agreement.

10. This Agreement constitutes the entire understanding of **The Parties** hereto related to the disclosure and protection of Sensitive Information and supersedes all prior or contemporaneous written or oral agreements or understandings.

11. This Agreement shall be construed in accordance with the laws of the State of Florida without regard to its conflict of law principles, and shall not be amended nor modified except by written instrument signed by both parties hereto.

IN WITNESS WHEREOF, **The Parties** hereto have caused this instrument to be executed in their names by their duly authorized and proper officials as designated below:

_____		**LDCC**	
Person:		Person:	######################
Title:		Title:	#######################
Address:		Address:	55 Battle Street The Town The City
Phone:		Phone:	012345677890
Date:		Date:	

BACKUP – PROCEDURE (For: A-17) - AUG 20XX – D23 – Issue 1

Introduction

This backup procedure has been developed to allow data essential to LDCC to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems.

In order to achieve this, a number of things need to be taken into account, such as:

a) copying of data to a medium which can then be stored in a secure place.

b) retrieval of data from the copy made on the medium.

c) secure storage of the media containing backup data.

d) recording of details about the media and what data it stores to facilitate the easy and correct identification of media when it is necessary to retrieve data from it.

e) testing the quality of the back-ups made by test retrieval of data.

f) who is responsible for completing the actions above

Back-up Procedure

These procedures cover all critical data and critical software contained on database and file servers within the five critical areas of the LDCC business as follows:

HR

Operations

Facilities

Finance

Sales and Marketing

The frequency of backups for each server, the media type used and the responsibility for carrying out the backups can be seen in the table below

Data to be Backed Up	Type	Frequency	Media	Responsibility
All critical HR Data and Software	Full	Weekly	Tape	Systems Admin
All critical Operations Data and Software	Full	Weekly	Tape	Systems Admin
All critical Facilities Data and Software	Full	Weekly	Tape	Systems Admin
All critical Finance Data and Software	Full	Weekly	Tape	Systems Admin
All critical Sales & Marketing Data and Software	Full	Weekly	Tape	Systems Admin

The weekly backup will be carried out as follows:

a) Retrieve the next tape in the sequence from the fire safe using the record of the last backup carried out as a guide
b) Check to ensure the tape is not damaged. If it is replace the tape with a new one and label accordingly.
c) Place the tape into the tape drive
d) Execute the backup process on the relevant server as per the schedule in ‘annex a’ of this procedure
e) Remove the tape from the tape drive
f) Label the tape with the name of the server backed up and the date
g) Store the tape at home (in a cool place i.e. garage)
h) Record details of the backup using the record template documented in ‘annex b’ of this procedure

In addition to the backups noted in the table above, a full backup will also be carried out of all critical data and software for each area on a quarterly basis as per the table below. These backups will be written to durable archive media and stored offsite for a period of no less than one year.

Data to be Backed Up	Type	Frequency	Media	Responsibility
All critical HR Data and Software	Full	Quarterly	DVD	Systems Admin
All critical Operations Data and Software	Full	Quarterly	DVD	Systems Admin
All critical Facilities Data and Software	Full	Quarterly	DVD	Systems Admin
All critical Finance Data and Software	Full	Quarterly	DVD	Systems Admin
All critical Sales & Marketing Data and Software	Full	Quarterly	DVD	Systems Admin

The quarterly archive backup will be carried out as follows:

a) Retrieve the next disk in the sequence from the offsite archive using the record of the last backup carried out as a guide
b) Check to ensure the disk is not damaged. If it is, replace it with a new one and label it accordingly
c) Place the disk in the disk drive of the relevant server as per the schedule in ‘annex a’ of this procedure
d) Execute the backup process for that server
e) Remove the disk from the server and return it to its case
f) Label the case with the server name and date
g) Arrange for the disk to be collected by secure courier and stored at the offsite archive
h) Record details of the backup using the record template documented in ‘annex b’ of this procedure

Back-up Media Handling

Two types of media are used for backups. Magnetic tape is used for the weekly full backups and DVD disks are used for quarterly archive backups as they are more durable than magnetic tape. All tapes will be labelled with the name of the server backed up, the date of the backup and a unique identifier so that it can be easily retrieved when necessary.

Weekly backup tapes are transported across the LDCC site in a protective plastic carry case. Tapes are to be stored at home (in a cool place i.e. garage)

Quarterly DVD backups when complete are returned to their individual cases and labelled to show the name of the server backed up, and the date the backup was carried out. Each DVD will also have a unique identifier so that it can be easily identified and retrieved when required.

Quarterly backups are then handed over to a secure courier to be transported to an offsite archive until required.

Back-up Restoration Testing

In order to ensure that backup media has not deteriorated and that all critical data and software has been successfully backed up, periodic restoration tests will be carried out in accordance with the schedule documented in ‘annex c’ of this procedure.

Two types of restoration test must be carried out (and indicated) as follows:

File recovery test – recover critical files from the backup in the case of loss or corruption of data on live systems as follows:

a) Recover tape from the fire safe
b) Insert the tape into the tape drive connected to the standby server
c) Recover data from tape into the database on the standby server
d) Ensure the data recovered from the tape matches data on the live server
e) Record details of the test using the form documented in ‘annex d’ of this procedure
f) Return the tape to the fire safe

System recovery test – recover the entire content onto a test server to ensure that systems can be recovered in the event of any unforeseen circumstances as follows:

a) Recover disk from offsite storage as per the schedule in ‘annex c’ of this procedure
b) Ensure standby server is operational and all previous recovered data has been removed
c) Recover data from archive disk onto the standby server
d) Check to ensure that all software is operational on the standby server
e) Check to ensure that data can be retrieved on the standby server
f) Record details of the test using the form documented in ‘annex d’ of this procedure
g) Return the disk to the offsite archive

Annex A – Backup Schedules

<table>
<tr><th colspan="5">WEEKLY BACKUP SCHEDULE</th></tr>
<tr><th>MONDAY</th><th>TUESDAY</th><th>WEDNESDAY</th><th>THURSDAY</th><th>FRIDAY</th></tr>
<tr><td>HR Full Backup</td><td>Facilities Full Backup</td><td>Sales and Marketing Full Backup</td><td>Operations Full Backup</td><td>Finance Full Backup</td></tr>
<tr><td colspan="5"></td></tr>
<tr><th colspan="5">QUARTERLY BACKUP SCHEDULE</th></tr>
<tr><td>HR</td><td>Facilities</td><td>Sales and Marketing</td><td>Operations</td><td>Finance</td></tr>
<tr><td>January Week 01</td><td>February Week 02</td><td>March Week 03</td><td>April Week 04</td><td>May Week 01</td></tr>
<tr><td>April Week 01</td><td>March Week 02</td><td>June Week 03</td><td>July Week 04</td><td>August Week 01</td></tr>
<tr><td>July Week 01</td><td>June Week 02</td><td>September Week 03</td><td>October Week 04</td><td>November Week 01</td></tr>
<tr><td>October Week 01</td><td>September Week 02</td><td>December Week 03</td><td>January Week 04</td><td>February Week 01</td></tr>
</table>

Annex B – Backup Log

This backup log should be completed daily to indicate the status of the backup scheduled for that day. At the end of the week the completed form should be stored in the IS Department

Day	Date	Time	Backup Type	System / Application Backed Up	Media Used.	Backup Status (Complete / Failed)	Carried out by:
Monday			Full	HR Database and File Server			
Tuesday			Full	Facilities Database and File Server			
Wednesday			Full	Sales and Marketing Database and File Server			
Thursday			Full	Operations Database and File Server			
Friday			Full	Finance Database and File Server			

Quarterly Backup Log (if applicable)

Date	Time	Server Name	Media Used.	Backup Status (Complete / Failed)	Carried out by:

Annex C – Backup Recovery Test Schedules

RECOVERY TEST ROTA FOR WEEKLY BACKUPS
One backup shall be selected from the completed weekly backups completed each week and tested in business unit rotation.

QUARTERLY BACKUP RECOVERY TEST SCHEDULE				
HR	Facilities	Sales and Marketing	Operations	Finance
January	March	May	July	September

Annex D – Backup Recovery Test Log

This backup recovery test log should be completed after every recovery test and the completed form should be stored in the IS Department

Recovery Test Type (weekly / quarterly)	**Date**	**Time**	**Business System Recovered**	**Media Used.**	**Backup Status (Complete / Failed)**	**Carried out by:**

Backup Log – D24 – Issue 3

This backup log should be completed daily to indicate the status of the backup scheduled for that day. At the end of the week the completed form should be stored in the IS Department

Day	Date	Time	Backup Type	System / Application Backed Up	Media Used.	Backup Status	Checked by:
Monday	27/10/xx	17:00	Full	HR Database and File Server	HR04	Complete	Graham Spring
Tuesday	28/10/xx	16:53	Full	Facilities Database and File Server	FA04	Complete	Graham Spring
Wednesday	29/10/xx	16:50	Full	Sales and Marketing Database and File Server	SM04	Complete	Graham Spring
Thursday	30/10/xx	16:28	Full	Operations Database and File Server	OP04	Complete	Graham Spring
Friday	31/10/xx	16:12	Full	Finance Database and File Server	FI04	Complete	Graham Spring

Quarterly Backup Log (if applicable)

Date	Time	Server Name	Media Used.	Backup Status (Complete / Failed)	Carried out by:
28/10/XX	16:55	Operations	OPD04	Failed	Graham Spring

Recovery Test Log (if applicable)

Date	Time	Server Name	Media Used.	Restore Status (Complete / Failed)	Carried out by:
31/10/xx	09:35	Finance Database and File Server	FI04	Complete	Geoff King

Backup Log – D24 – Issue 1

This backup log should be completed daily to indicate the status of the backup scheduled for that day. At the end of the week the completed form should be stored in the IS Department

Day	Date	Time	Backup Type	System / Application Backed Up	Media Used.	Backup Status	Checked by:
Monday	01/09/xx	17:00	Full	HR Database and File Server	HR01	Complete	Graham Spring
Tuesday	02/09/xx	16:53	Full	Facilities Database and File Server	FA01	Complete	Graham Spring
Wednesday	03/09/xx	16:50	Full	Sales and Marketing Database and File Server	SM01	Complete	Graham Spring
Thursday	04/09/xx	16:28	Full	Operations Database and File Server	OP01	Failed	Graham Spring
Friday	05/09/xx	16:12	Full	Finance Database and File Server	FI01	Complete	Graham Spring

Quarterly Backup Log (if applicable)

Date	Time	Server Name	Media Used.	Backup Status (Complete / Failed)	Carried out by:
03/09/XX	16:55	Sales & Marketing	SMD01	Complete	Graham Spring

Recovery Test Log (if applicable)

Date	Time	Server Name	Media Used.	Restore Status (Complete / Failed)	Carried out by:
01/09/xx	09:35	HR Database and File Server	HR01	Complete	Graham Spring

Backup Log – D24 – Issue 1

This backup log should be completed daily to indicate the status of the backup scheduled for that day. At the end of the week the completed form should be stored in the IS Department

Day	Date	Time	Backup Type	System / Application Backed Up	Media Used.	Backup Status	Checked by:
Monday	03/11/xx	17:00	Full	HR Database and File Server	HR02	Complete	Graham Spring
Tuesday	04/11/xx	16:53	Full	Facilities Database and File Server	FA02	Complete	Graham Spring
Wednesday	05/11/xx	16:50	Full	Sales and Marketing Database and File Server	SM02	Complete	Graham Spring
Thursday	06/11/xx	16:28	Full	Operations Database and File Server	OP02	Failed	Graham Spring
Friday	07/11/xx	16:12	Full	Finance Database and File Server	FI02	Complete	Graham Spring

Quarterly Backup Log (if applicable)

Date	Time	Server Name	Media Used.	Backup Status (Complete / Failed)	Carried out by:
03/11/XX	16:55	Finance	FID02	Complete	Graham Spring

Recovery Test Log (if applicable)

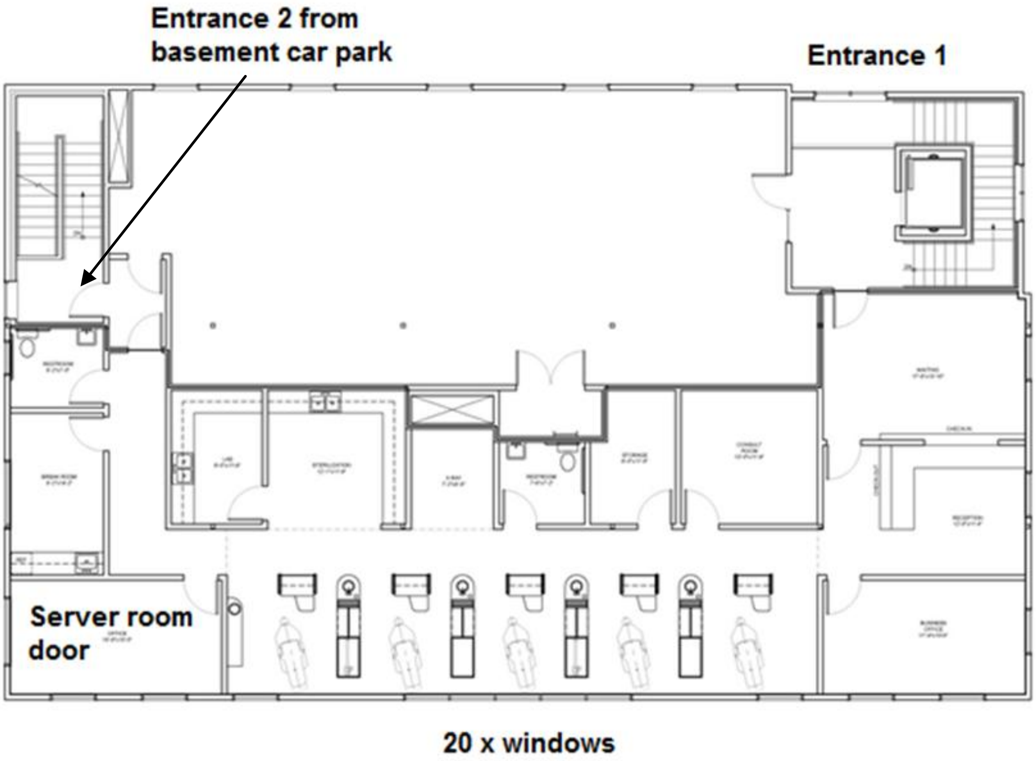
Date	Time	Server Name	Media Used.	Restore Status (Complete / Failed)	Carried out by:
06/11/xx	09:35	Operations	OP02	Failed	Graham Spring

Physical Entry Controls Procedure for: EI-6 (Physical Location) – OCT 20XX – D25 – Issue 2

Introduction

LLDC provides operational cover for its clients on a 24/7/365 basis, consequently access to its offices needs to be available at all times. All staff (including temporary and contract staff) are issued with an access card to the building and any areas within the building to which they have authorised access. This card includes a photograph and must be worn by members of staff at all times when they are in the offices.

Visitors (including maintenance and service engineers, etc.) are provided with a visitor card which provides limited access to areas within the offices and they must be accompanied at all times whilst inside the building.



Staff Access

All staff must present their card to the building access card reader upon entering and leaving the building, failure to do this is a disciplinary offence and will be dealt with in accordance with the company's disciplinary procedure.

Access cards - Issuing

When first starting work at LLDC, staff will be provided with a temporary card in order to access the building. HR will complete form HR2 (Access Change Form) and send to Facilities during this period requesting a photo-ID card. During the initial induction session with HR they will be then issued with their photo-ID card and sign to acknowledge its receipt on the same form (HR2). The temporary card will be returned to reception by HR. See card issuing record BI – 1. Name of staff to be issued and the card number is to be recorded.

Lost or Forgotten Cards

In the event that a member of staff forgets their access card, a temporary one will be issued by the Receptionist (or Shift Manager if applicable). This must be handed back to the Receptionist/Shift Manager at the end of the shift.

In the event of a card being lost a temporary card is to be issued using the same process as above and an email must be sent to the Facilities Manager and the member of staff's line manager in order that a replacement can be issued and the lost card deactivated.

Temporary cards will be linked to the individual in order to maintain the link to the payroll system. See card issuing record BI – 1. Name of staff to be issued and the card number is to be recorded.

Access to secure areas

If access is required to specific secure areas (e.g. computer room) this must be authorised by a named individual. In addition, every three months the manager responsible for the secure area must be provided with a list of staff that have access for review and sign-off.

Staff Termination

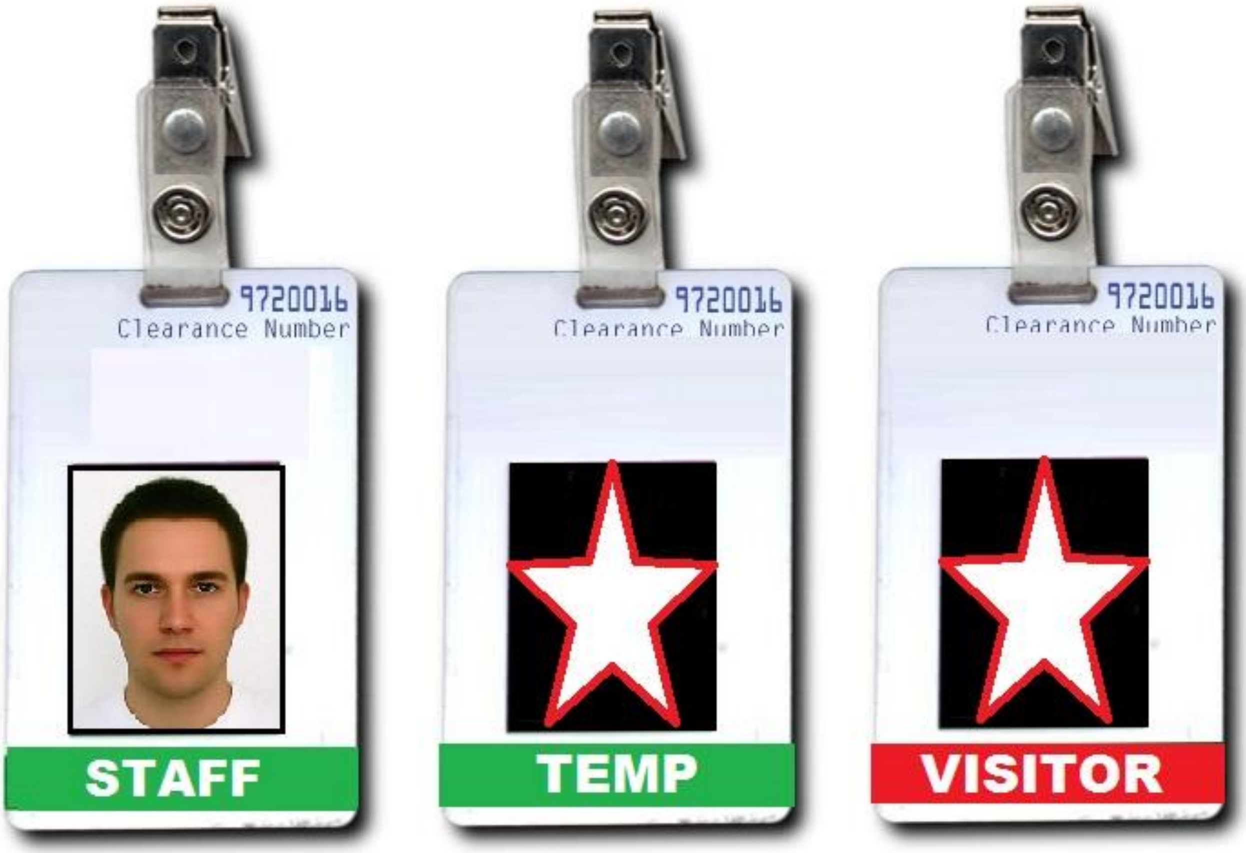
When staff (temporary or contract) leave the employment of LLDC HR must complete form HR2 (Access Change Form). This is to notify the Facilities department in order that the associated access card can be disabled. The time limit for this activity is six months after termination.

Visitor Access

All visitors must complete the 'Visitor Book' upon arrival at the offices and issued with a numbered 'Visitor' card. They should be permitted unaccompanied access to the offices. Under no circumstances should visitors be provided access to the MD's office.

Upon leaving the offices the Visitor card should be handed back to reception and form BI 1 noted with this.

LDCC access Cards



IT Server room lock

BI 1 TEMPORARY ACCESS CARDS

Date	Name (BLOCK CAPITALS)	Department	Card No	Car Registration	Returned (Date/Inits)

LDCC HR2 Access Change Form

NAME	
JOB TITLE	
APPROVED BY	

TASK	DATE REC’D/ COMPLETED	COMMENTS (if any)
CHANGE REQUIREMENTS		
SPECIFY:		
Access Card		
Current Security Level of Access SPECIFY:		
Requested new Security Level of Access SPECIFY:		
Deactivation of Security Level of Access? – Yes or No		
Reason for change (please specify):		
Access Card updated and reissued or sent for deactivation		
Received by: Signature:		
Completing HR Manager:		

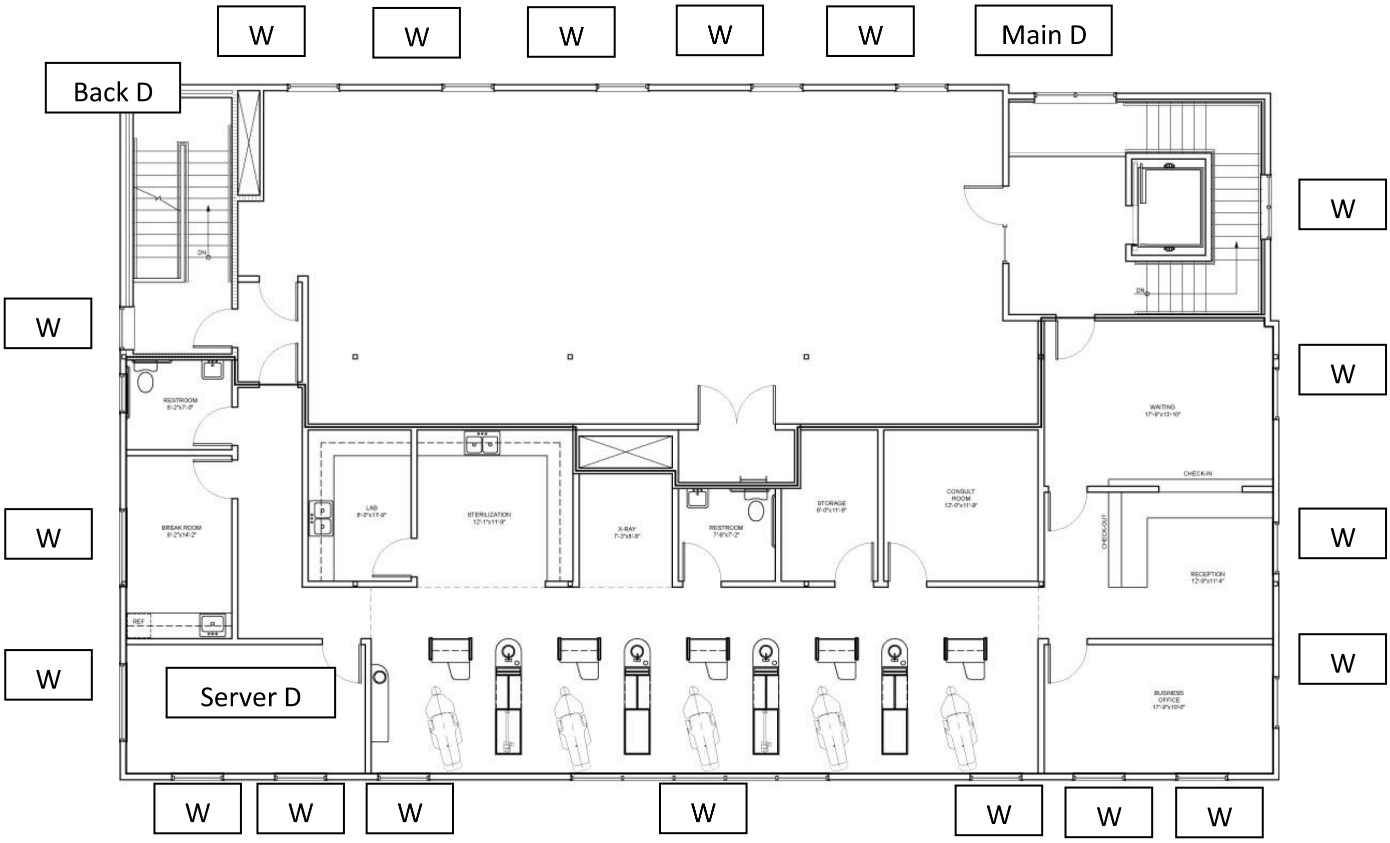
The Lock
Company

Pink Street

The Town

Access review 16/07/20xx

D26 – Issue 1



Notes:

19 insecure window locks identified
3 insecure door locks identified

Recommendation:

Replace all window locks
Replace all external door locks with fit card access system.
Server room to have combination lock

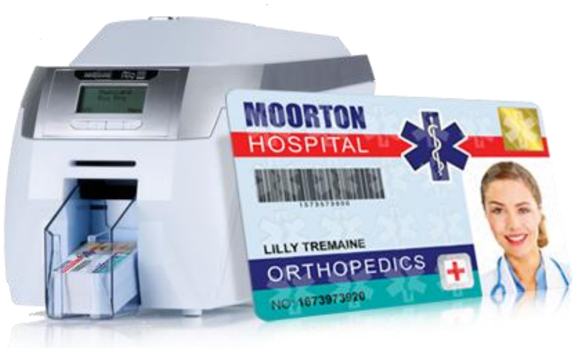
LDCC

The Printer Company

Pink Street

The Town

INVOICE



Invoice Number: 54321

Card Printer Invoice – D27 - Issue 1

Invoice Date: 22/09/xx

Order Information:

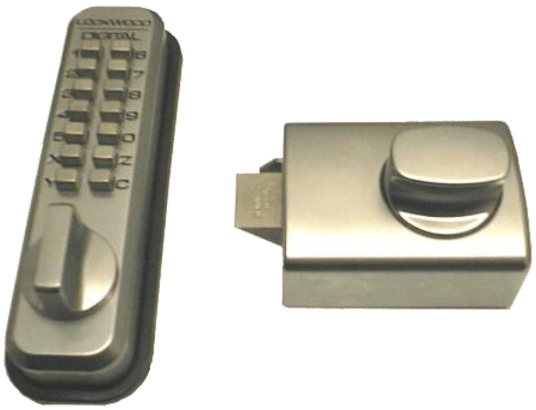
Qty	Product Description	Amount Each	Amount
1	Colour magnetic card printer	£1234	£1234
500	Card blanks	£145	£145
		Subtotal:	
		Tax:	
		Shipping:	
		Grand Total:	**£1,379**

Notes:
Card printer delivered and installed complete with product training

The Lock
Company

Pink Street

The Town



INVOICE

Doors and Windows Invoice D27-Issue 1

Invoice Number: 54321

Invoice Date: 22/09/xx

Order Information:

Qty	Product Description	Amount Each	Amount
44	Window locks	£33	£396
2	Button locks	£145	£290
34	Door Locks	£55	£1870
2	Key station	£45	£90
		Subtotal:	
		Tax:	
		Shipping:	
		Grand Total:	**£2,646**

Notes:
Window locks installed Door locks installed Combination button lock on IT door

…making excellence a habit.™

VISITOR BOOK (extract) – D28 – Issue 1

Date	Name	Company	To See	Card No	Time in	Time out	Car Registration (if you don't mind)
12/11/XX	Kaylene Upchurch	Indian Gas	Clive Page	01	10.00	12.12	-
12/11/XX	Rasheeda Guerro	Government Office (Data protection enforcement)	Mr Swan		10.10	12.34	-
12/11/XX	Tam Sowa	Raj Security	Clive Page	03	11.24	16.34	-
12/11/XX	Staci Fudge	Data Centre Express		01	12.44	13.55	-
12/11/XX	Rudolph Fentress	Cloud Security	Chris Flood	05	14.22	17.00	-
12/11/XX	Nicol Husman	Facilities are us	Simon Lock	06	15.02	17:00	-
12/11/XX	Renata Mcgrane	Let me in	Jos Taylor	08	15.32		-
12/11/XX	Marlyn Martello	Security Ha	Kayla Norman	03	15.34	16.12	-
12/11/XX	Kathline Grass	Integrity what's that	Clive Page	01	16.05	17:00	-
12/11/XX	Eleonore Purser	Availability all the time	Teddy Armstrong	02	16.15		-
12/11/XX	Angelo Lamarche	Police (Warrant)	Mr Swan		16.55	23:59	-

TEMPORARY ACCESS CARDS – D29 – Issue 1

Date	Name (BLOCK CAPITALS)	Department	Card No	Signature	Returned (Date/Inits)
19/10/xx	Sarah Pippins	HR	001	Sarah Pippins	20/10/xx
20/10/XX	Tracey Baker	HR	009	Tracey Baker	25/10/XX
20/10/XX	Gordon Black	Controls Assurance	006	Gordon Black	25/10/XX
23/10/XX	John Bishop	IT	003	John Bishop	23/10/XX
27/10/XX	Teddy Armstrong	Operations	001	Teddy Armstrong	
28/10/XX	Fay Woodward	Operations	009	Fay Woodward	09/11/XX
01/11/XX	Michael Hamilton	Operations	005		30/11/XX
01/11/XX	Ian Smith	Operations	006	Ian Smith	05/11/XX
04/11/XX	Anthony Summer	Operations		Anthony Summer	07/11/XX
05/11/XX	Debbie Cockram	Operations	004	Debbie Cockram	07/11/XX
05/11/XX	Amanda French	Operations	008	Amanda French	10/11/XX
08/11/XX	Rodney Trotter	Finance	002	Rodney Trotter	10/11/XX
09/11/XX	Visitor	To see Finance	002	James Spec	

Authorised Managers List – D30 – Issue 1

The table below contains the names of individuals who are authorised to grant access to LDCC information assets, buildings and information processing facilities.

This list shall be reviewed periodically by senior management.

Name	Department	Position
Alan Swan	Executive	MD/CEO
Peter Gaut	Executive	Resource Director
Clive Prichard	IT	IS Manager/Management representative for ISMS
Joe Cullum	Executive	Chief Operations Officer
Carly Hudd	Executive	Finance Director
Simon Lock	Facilities	Facilities Manager
Amanda French	Operations	Operations Manager
Reggie Gates	Operations	Phone Operative
John Bishop	IT	IT Team Leader / Manager

Data Centre Authorised Staff List – D31- Issue 1

The table below contains the names of individuals who are authorised to have access to the LDCC data centre (computer room) along with details of who the access was approved by.

This list shall be reviewed quarterly by the Computer Operations Manager to ensure it remains accurate and up to date.

Name	Department	Position	Authorised By	Date
Clive Prichard	IT	IS Manager/Management representative for ISMS	IT Manager	26/10/XX
Graham Spring	IT	Analyst/Systems Admin	IS Manager	18/08/XX
Colin Strange	IT	Analyst	IT Manager	02/11/XX
Simon Lock	Facilities	Facilities Manager	IT Manager	17/05/XX
Geoff King	Facilities	Maintenance Engineer	IT Manager	15/01/XX
Chris Flood	IT	Analyst	IT Manager	17/03/XX
Gordon Black	Controls Assurance	ISMS Auditor	IT Manager	01/10/XX
John Bishop	IT	Team Leader/Manager	MD / CEO	09/11/XX

LDCC HR2 Access Change Form – D32 – Issue 1

NAME	Amanda Lomond
JOB TITLE	Phone Operative
APPROVED BY	Simon Lock (Facilities Manager)

TASK	DATE REC’D/ COMPLETED	COMMENTS (if any)
CHANGE REQUIREMENTS		
SPECIFY: New Starter	Oct 20XX	
Access Card		
Current Security Level of Access SPECIFY:	None	
Requested new Security Level of Access SPECIFY:	Basic	
Deactivation of Security Level of Access? – Yes or No	NO	
Reason for change (please specify): As above		
Access Card updated and reissued or sent for deactivation	Nov 20XX	
Received by: Amanda French Signature: **Amanda French**	Nov 20XX	
Completing HR Manager: Sarah Pippins	Nov 20XX	

LDCC HR2 Access Change Form – D32 – Issue 1

NAME	Clive Page
JOB TITLE	Sales Manager/Acting Sales Director
APPROVED BY	Raj Patel (HR Director)

TASK	DATE REC'D/ COMPLETED	COMMENTS (if any)
CHANGE REQUIREMENTS		
SPECIFY: Left the Organization	Nov 20XX	
Access Card		
Current Security Level of Access SPECIFY:	Access to Data Centre/Computer Room	
Requested new Security Level of Access SPECIFY:	Remove all access	
Deactivation of Security Level of Access? – Yes or No	YES	
Reason for change (please specify): As above	LEFT	
Access Card updated and reissued or sent for deactivation	(Got six months)	
Received by: Signature:	N/A	
Completing HR Manager: Sarah Pippins		

LDCC HR2 Access Change Form – D32 – Issue 1

NAME	Graham Spring
JOB TITLE	Analyst/Systems Admin
APPROVED BY	IT Manager – John Bishop

TASK	DATE REC'D/ COMPLETED	COMMENTS (if any)
CHANGE REQUIREMENTS		
SPECIFY: Needs access to enable backups	Aug 20XX	
Access Card		
Current Security Level of Access SPECIFY:	Basic	
Requested new Security Level of Access SPECIFY:	Access to Computer Room	
Deactivation of Security Level of Access? – Yes or No	NO	
Reason for change (please specify): As above		
Access Card updated and reissued or sent for deactivation	Aug 20XX	
Received by: Graham Spring Signature: Graham Spring	Aug 20XX	
Completing HR Manager: Sarah Pippins	Aug 20XX	

FOR: ‘II – 11 Human Resources Security (Screening Control)’ June 20xx

Human Resource Security Screening Policy – D33 – Issue 2

A.7.1Prior to Employment

7.1.1 Screening

A. Prospective Employee Information

Personal information about a prospective employee may not be gathered unless it is necessary to make an employment decision and relevant to the job.

For all appointments the organisation shall undertake screening prior to employment that includes:

- Name
- Address
- Nationality (passport or proof of naturalisation)
- Marital status
- Education and qualifications
- Previous Employment
- Criminal record declaration and spent convictions
- Two references (including at least one previous employer)

All staff should expect that they will undertake Government standard security clearance and must be given opportunity to disclose any reason why they believe they may not be able to attain such clearance prior to employment.

Additional background checks may be undertaken if required for the performance of a specific role or at the request of a client. Such checks may include off-hours activities, political affiliations, performance on previous jobs, credit history, examination of criminal conviction records, lawsuit records, credit bureau records, driver’s license records and other personal details.

B. Accessing Private Information

To prevent unnecessary and inappropriate disclosures, only those staff members who pass a background check will be granted access to private information.

Temporaries, consultants, contractors, and outsourcing organisation staff must not be given access to sensitive information, or be allowed to access critical information systems, unless they have gone through a background check commensurate with the background checks given to regular employees.

FOR: ‘II – 11 Human Resources Security (Screening Control)’ July 20xx

Screening Procedure – D34 – Issue 1

1.0 Purpose

The purpose of this document is to provide a structured procedure for screening new employees. The primary objective of the procedure is to safeguard our information and financial assets.

The organisation is committed to the maintenance of high levels of confidentiality and integrity. This procedure supports that commitment by establishing a consistent approach to screening.

The requirement for implementation of these screening procedures is assessed against the risks to the organisation, these risks are assessed and periodically reviewed by Senior Management.

1.2 Specific Instructions, tactics, methods, practices and procedures

There are two types of vetting procedure:

i) Basic Check - generic new employee screening
ii) Additional Checks - role or client specific screening

2.0 Basic Check

Where an individual applies for a role within the organisation, Human Resources will send the applicant a Basic Check form.

A ‘Basic Check’ is a procedure to assure the identity and reliability of prospective members of staff

A ‘Basic Check’, applies to Recruitment Vetting, and requires applicants to prove their identity and any ‘spent convictions’

The Basic Check process comprises three stages that should be carried out in the order shown. Between each stage the information collected should be reviewed and assessed. The stages are as follows:

- Identity Check
    - Name
    - Address
    - Nationality (passport or proof of naturalisation)
    - Marital status
- References
    - Education and qualifications
    - Verification of previous employment
    - Two references (including at least one previous employer)
- Criminal Record Declaration
    - Criminal record declaration and spent convictions

2.1 Identity Check

Correctly identifying an individual is a fundamental aspect of the screening process

In addition to the basic check form, proof of identity will be confirmed, as below by the relevant Human Resources Advisor. Employment law differs from country to country so nationality of the individual is valuable. In all cases, individuals must provide original documents.

2.1.1 Documents to be provided

Full 10 year passport, National Identity Card or two of the following:

- Driving Licence
- Previous employment records or tax forms
- Birth Certificate – issued within 6 weeks of birth
- Cheque book and bank card – with 3 statements and proof of signature
- Credit card – with photograph of the individual
- Proof of residence – such as a council tax, gas, electricity, water or telephone bill

The following documents **must not** be accepted as proof of identity:

- Duplicate or photocopied identity documents – modern photocopiers can often produce excellent results;
- An international driving licence – easily and frequently forged;
- Copy Birth certificate issued more than 6 weeks after birth – can be purchased on request for any individual without proof of identity;
- Forces ID Card
- Library Card
- Mobile phone bill
- Marriage certificate
- Provisional Driving Licence

In some cases, particularly where young individuals are concerned, such documents may not be available to prove identity. Where this appears to be a genuine problem, the individual should be asked to supply a passport-sized photograph endorsed on the back with the signature of a person of someone standing in the community, for example a medical practitioner, officer of the armed forces, clergyman, teacher, lecturer, lawyer, bank manager, or civil servant. The signatory should have known the individual for a minimum of three years. This should be accompanied by a signed statement from the signatory giving their full name, address and telephone number, and confirming the period of that they have known the individual.

2.2 References

Appropriate references can provide a high level of assurance, particularly where the reference is given by a reputable organisation. Reasonable steps should be taken to ensure that the reference and the references are genuine, especially where the reference is less than convincing, for example, being written on poor quality paper or containing spelling or grammatical errors.

At least one of the references required should be the individual’s most recent employer and should cover a period of one year or, from a previous employer for the same period. If an employer's reference is not available, a personal or academic reference should be obtained. The relevant Human Resources Advisor will check the references of an individual.

2.3 Criminal Convictions

Convictions will be detailed on the Basic Check Form and a check on criminal records will be made as part of the formal screening process. Criminal Record checks will then be undertaken with relevant authorities. The Human Resources Advisor will be responsible for managing the completion of the necessary security checks on applicants for organisation positions.

If any traces are found on the applicant whilst carrying out the security checks, the Human Resources Advisor will refer these to the HR Manager or the Resources Director, who will then make a decision on whether the relevant conviction will bar the applicant from employment with the organisation

3.0 Additional Checks

3.1 Risk Assessment

For specific privileged roles or roles where the customer has a higher screening requirement than met by the basic checks completed for all staff, Senior Management must be informed and appropriate risk assessment undertaken. Dependent of the specific requirement or assessed business risk the following screening checks may be required:

- Counter terrorist checks
- National security clearances
- Additional criminal record checks
- Credit reference agency checks, for:
  - any undisclosed accounts;
  - default accounts;
  - county court judgements;
  - attachment of earnings orders:
  - voluntary agreements; and / or
  - bankruptcy

3.2 Requesting Additional Checks

The hiring manager must complete and submit an Additional Security Checks Requirement form to the Human Resources Department. This will detail the checks that are required and the frequency for review of those checks. Each review period will be treated as a new screening process as screening for security clearances are based on a snap shot in time, they do not provide a guarantee of future reliability.

The HR Advisor will issue the employee with an Additional Security Checks Form for completion.

All additional screening requirement factors will be assessed by the Human Resources Manager. Any irregular findings will be referred to the Resources Director.

Whilst individual factors may not in themselves justify a decision to refuse, limit or withdraw clearance, a combination of factors may do so. The Resources Director will review the case and make a decision as to whether to grant clearance or not.

The front of the Additional Security Checks form will be stamped CLEARED or REFUSED and signed by the HR Manager or Resources Director and inserted into the employee's HR file.

All refusals will be fully documented with the rationale for the decisions.

4.0 Refusal of Screening Clearance

If clearance is refused, individuals will be informed, and where possible, provided with an explanation. However, there may be circumstances, for example in cases where notification could prejudice a criminal or disciplinary inquiry, or when disclosure would breach the Data Protection Act or other legislation, where information may be withheld. In addition, information may have been provided by third parties, in confidence, during vetting inquiries. Such information will only be disclosed to the subject if the person who has provided the information agrees to its disclosure.

4.1 Withdrawal of a Vetting Clearance

There may be cases when an individual’s clearances will have to be withdrawn. This may be done following a review of changes of circumstances, following a disciplinary process or if any other adverse information comes to light concerning the individual. All information will be assessed against the required screening factors

Before a decision is made to withdraw a vetting clearance a risk assessment will be conducted by the Resources Director and the justification for the withdrawal documented.

5.0 Reporting Change

All employees are responsible for informing the organisation is writing of any change to their personal circumstances that may affect their employment to the Human Resources Department.

6.0 Consent

Applicants for security clearance should fully understand and consent to the process-taking place. Consent can be signified by an individual completing a declaration agreeing to the procedure.

In the application of this procedure, the organisation will not discriminate against any persons regardless of age, gender, transgender, sexual orientation, disability, race, colour, language, religion, political, or other opinion, national or social origin, association with national minority, property

LDCC Basic Check Screening Form

This basic check screening form must be completed for all individuals who apply for a role at LDCC. All information provided will be verified by a human resources advisor on your first day of work should your application be successful. Please note that you will be required to bring ***original documents*** with you on your first day for this verification to be completed. Photocopies of documents will not be accepted.

Acceptable forms of identification for a British national are as follows:

Full 10 Year Passport
Birth Certificate (issued within six weeks of birth)
Cheque book and bank card with three accompanying statements and proof of signature
Credit card with photograph
Utility bills (electricity, telephone, gas, water)
Council tax bill.

Please note that the following are NOT ACCEPTED as proof of identification:

International driving licenses

Copy of birth certificate issued more than six weeks after birth
Forces ID card
Library card
National Insurance number
Mobile telephone bill
Marriage certificate
Provisional driving license

IDENTITY CHECK Please confirm the following information:	
Your Full Name	
Your Full Address	
Your Nationality	
Your Marital Status	
REFERENCES	
Please provide the name and address of at least two referees, one of which should be your most recent employer.	
REFERENCE 1	
Name:	
Address:	
Telephone Number:	
Relationship to you:	
REFERENCE 2	
Name:	
Address:	
Telephone Number:	
Relationship to you:	
Please provide details of your education and any relevant professional qualifications.	

CRIMINAL RECORDS DECLARATION (Complete only one section)

I HAVE NO CONVICTIONS, WHETHER SPENT OR UNSPENT, CAUTIONS, REPRIMANDS, OR FINAL WARNINGS.

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature ……………………………………………….(Applicant)   Date

I HAVE THE FOLLOWING CONVICTIONS, CAUTIONS, REPRIMANDS AND/OR FINAL WARNINGS: (record below details of any and all convictions, whether spent or unspent, cautions, reprimands and / or final warnings that you may have to declare)

………
.………………………………………
………
…………………………………………

…making excellence a habit.™

……

……

……

……

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature……………………………………………… (Applicant) Date …./……/……

Please note that all employees should expect to undertake Government standard security clearance. If you believe you will not be able to attain such clearance then please indicate below the reason for this.

I believe I may not be able to attain Government standard security clearance because:

THE FOLLOWING SECTION IS TO BE COMPLETED BY HR

EVIDENCE SEEN	DATE SEEN
IDENTIFICATION	
EDUCATION AND QUALIFICATIONS – CERTIFICATES SEEN (if any)	
REFERENCES	
Reference 1 Verified **YES** / NO (delete or highlight as applicable)	
Reference 2 Verified **YES** / NO (delete or highlight as applicable)	
If references were not able to be verified or were not available please enter details here regarding why this is the case:	
Checked by:	Signature:

…making excellence a habit.™

LDCC HR3 Additional Check Screening Form

The individual named below requires additional screening check to be completed as a condition of their employment with LDCC. In addition, a formal statement is required outlining the risks (if any) that these additional checks have highlighted in the context of the position applied for.

Applicant Name:			
Position Applied For			
Additional Checks Requested by			
Start Date (if known)		Checks to be completed before start?	Y/N
Checks Requested (delete those not required)	Credit	Criminal	Government security clearance

Credit check

Reference provider: ……………………………………………………………………………………………

Date requested: ………………………… Date reply received: …………………………………..

Check	Result	Comments
Undisclosed accounts		
Accounts in default		
CCJs		
Voluntary Agreements		
Bankruptcy		

Criminal Record

Check	Result	Comments

Government Security Clearance

Date Clearance form submitted: …………………………………………

Date result received: ………………………………………………

Result: Confirmed/Declined

NAME	Amanda French
JOB TITLE	Operations Manager
DEPARTMENT	Operations
START DATE	23/04/09
REPORTING TO	MD / CEO
APPROVED BY	MD / CEO

LDCC HR1 Starter/Leavers Form – D35 – Issue 1

TASK	DATE REC'D/ COMPLETED	COMMENTS (if any)
ONBOARDING		
HR file created	21/04/09	
CV enclosed	21/04/09	
JD enclosed	21/04/09	
Selection process documentation enclosed	21/04/09	
Offer letter and screening pack sent out	21/04/09	
Completed screening pack received	22/04/09	
BASIC CHECK		
Basic Check Form completed	22/04/09	
Proof of Nationality	23/04/09	
Proof of Marital Status	23/04/09	
Education check completed	23/04/09	
Qualifications verified	23/04/09	
Reference 1 obtained and satisfactory	30/04/09	
Reference 2 obtained and satisfactory	01/05/09	
Previous employment checked		
Criminal record and spent convictions form completed		
ADDITIONAL CHECKS – Required Y/N	No	
SPECIFY:	N/A	
Contract sent out	21/04/09	

Contract signed and received	23/04/09	
Holiday entitlement calculated and added to DB	21/04/09	
P45 received	23/04/09	
Start date confirmed	21/04/09	
NEW STARTER REQUIREMENTS		
ICT Request Form completed	22/04/09	
Security Level of Access SPECIFY: Standard	22/04/09	
Security Level of Access APPROVED BY: MD /CEO	22/04/09	
SMART Card issued		
Identification Badge created, photo taken and badge issued	23/04/09	
Induction Checklist completed	23/04/09	
Benefits Form	23/04/09	
LEAVER REQUIREMENTS		
ICT return form completed		
Security Level of Access to be de-activated SPECIFY:		
Security Level of Access (deactivation) sent to Physical Security Mger		
SMART Card returned		
SMART Card (deactivation) sent to Physical Security Mger		
Identification Badge returned		
Leavers Checklist completed		
Completing HR Manager:		

NAME	Graham Spring
JOB TITLE	IT Analyst
DEPARTMENT	IT
START DATE	18/01/11
REPORTING TO	IT Manager
APPROVED BY	IT Manager

LDCC HR1 Starter/Leavers Form – D35 – Issue 1

TASK	DATE REC'D/ COMPLETED	COMMENTS (if any)
ONBOARDING		
HR file created	10/01/11	
CV enclosed	10/01/11	
JD enclosed	10/01/11	
Selection process documentation enclosed	10/01/11	
Offer letter and screening pack sent out	22/12/10	
Completed screening pack received	10/01/11	
BASIC CHECK		
Basic Check Form completed	18/01/11	
Proof of Nationality	18/01/11	
Proof of Marital Status	18/01/11	
Education check completed	15/12/10	
Qualifications verified	15/12/10	
Reference 1 obtained and satisfactory	25/1/11	
Reference 2 obtained and satisfactory		
Previous employment checked	N/A	
Criminal record and spent convictions form completed	18/01/11	
ADDITIONAL CHECKS – Required Y/N	No	
SPECIFY:	N/A	

Contract sent out	22/12/10	
Contract signed and received	3/01/11	
Holiday entitlement calculated and added to DB	15/01/11	
P45 received	N/A	
Start date confirmed	4/01/11	
NEW STARTER REQUIREMENTS		
ICT Request Form completed	15/01/11	
Security Level of Access SPECIFY: IT Admin	15/01/11	
Security Level of Access APPROVED BY: IS Manager	15/01/11	
SMART Card issued	18/01/11	
Identification Badge created, photo taken and badge issued	18/01/11	
Induction Checklist completed	25/01/11	
Benefits Form	19/01/11	
LEAVER REQUIREMENTS		
ICT return form completed		
Security Level of Access to be de-activated SPECIFY:		
Security Level of Access (deactivation) sent to Physical Security Mger		
SMART Card returned		
SMART Card (deactivation) sent to Physical Security Mger		
Identification Badge returned		
Leavers Checklist completed		
Completing HR Manager:		

NAME	Yan Kypers
JOB TITLE	Phone Operative
DEPARTMENT	Operations
START DATE	02/09/12
REPORTING TO	Operations Team Leader
APPROVED BY	Operations Manager

LDCC HR1 Starter/Leavers Form – D35 – Issue 1

TASK	DATE REC'D/ COMPLETED	COMMENTS (if any)
ONBOARDING		
HR file created	25/08/12	
CV enclosed	25/08/12	
JD enclosed	25/08/12	
Selection process documentation enclosed	25/08/12	
Offer letter and screening pack sent out	08/08/12	
Completed screening pack received	10/08/12	
BASIC CHECK		
Basic Check Form completed	25/08/12	
Proof of Nationality	02/09/12	
Proof of Marital Status	02/09/12	
Education check completed		
Qualifications verified	02/09/12	
Reference 1 obtained and satisfactory	27/08/12	
Reference 2 obtained and satisfactory		
Previous employment checked	25/08/12	
Criminal record and spent convictions form completed	10/08/12	
ADDITIONAL CHECKS – Required Y/N	No	
SPECIFY:	N/A	
Contract sent out	14/08/12	

Contract signed and received	18/08/12	
Holiday entitlement calculated and added to DB	25/08/12	
P45 received	02/09/12	
Start date confirmed	20/08/12	
NEW STARTER REQUIREMENTS		
ICT Request Form completed	29/08/12	
Security Level of Access SPECIFY: Basic	29/08/12	
Security Level of Access APPROVED BY: Operation Manager	29/08/12	
SMART Card issued	02/09/12	
Identification Badge created, photo taken and badge issued	02/09/12	
Induction Checklist completed	10/10/12	
Benefits Form	02/09/12	
LEAVER REQUIREMENTS		
ICT return form completed		
Security Level of Access to be de-activated SPECIFY:		
Security Level of Access (deactivation) sent to Physical Security Mger		
SMART Card returned		
SMART Card (deactivation) sent to Physical Security Mger		
Identification Badge returned		
Leavers Checklist completed		
Completing HR Manager:		

LDCC Basic Check Screening Form – D36 – Issue 2

This basic check screening form must be completed for all individuals who apply for a role at LDCC. All information provided will be verified by a human resources advisor on your first day of work should your application be successful. Please note that you will be required to bring ***original documents*** with you on your first day for this verification to be completed. Photocopies of documents will not be accepted.

Acceptable forms of identification for a British national are as follows:

Full 10 Year Passport

Birth Certificate (issued within six weeks of birth)

Cheque book and bank card with three accompanying statements and proof of signature

Credit card with photograph

Utility bills (electricity, telephone, gas, water)

Council tax bill.

Please note that the following are NOT ACCEPTED as proof of identification:

International driving licenses

Copy of birth certificate issued more than six weeks after birth

Forces ID card

Library card

National Insurance number

Mobile telephone bill

Marriage certificate

Provisional driving license

IDENTITY CHECK Please confirm the following information:	
Your Full Name	Amanda French
Your Full Address	21 Great Marlborough Street London W1F 7HL

Your Nationality	British
Your Marital Status	Married
REFERENCES	
Please provide the name and address of at least two referees, one of which should be your most recent employer.	
REFERENCE 1	
Name:	Kevin D. Beatty
Address:	Brookfield Engineering 39 Floral Street London WC2E 9DG
Telephone Number:	0207 379 8678
Relationship to you:	Line Manager
REFERENCE 2	
Name:	Paula D. Corso
Address:	PDC Electronics 43 Bow Lane London EC4M 9DT
Telephone Number:	0208 735 1000
Relationship to you:	Line Manager
Please provide details of your education and any relevant professional qualifications.	4 GCSE's from Marlborough High School
CRIMINAL RECORDS DECLARATION (Complete only one section)	
I HAVE NO CONVICTIONS, WHETHER SPENT OR UNSPENT, CAUTIONS, REPRIMANDS, OR FINAL WARNINGS.	

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature ………Amanda French……………………………………….(Applicant)   Date 17/04/2009

I HAVE THE FOLLOWING CONVICTIONS, CAUTIONS, REPRIMANDS AND/OR FINAL WARNINGS:

(record below details of any and all convictions, whether spent or unspent, cautions, reprimands and / or final warnings that you may have to declare)

……….
………………………………

………
………………………………

………
………………………………

………
………………………………

………
………………………………

………
………………………………

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature……………………………………………… (Applicant)   Date …./……/……

Please note that all employees should expect to undertake Government standard security clearance. If you believe you will not be able to attain such clearance then please indicate below the reason for this.

I believe I may not be able to attain Government standard security clearance because:

THE FOLLOWING SECTION IS TO BE COMPLETED BY HR	
EVIDENCE SEEN	DATE SEEN
IDENTIFICATION	
Full British driving license	23/04/09
Library Card	23/04/09
EDUCATION AND QUALIFICATIONS – CERTIFICATES SEEN (if any)	
None	23/04/09
REFERENCES	
Reference 1 Verified **YES** / NO (delete or highlight as applicable)	30/04/09
Reference 2 Verified **YES** / NO (delete or highlight as applicable)	01/05/09
If references were not able to be verified or were not available please enter details here regarding why this is the case:	
Checked by: Sarah Pippins	Signature: SARAH PIPPINS

The Council

To: Whomever it may concern

Subject: Reference for Amanda Frecher

Dear Sir / Madam,

In response to your request for a reference for Ms Amanda Frecher.

I can confirm that Ms Amanda Frecher was employed as a Customer Services Administrator in the Housing Department of the Council from November 2006 to Jan 2009.

Her attendance record during her time with the Council was good, and that was about all.

Yours faithfully

Titilayo Okunola

HR Administrator

P.D.C. ELECTRONICS

43 Bow Lane, London, EC4M 9DT

Reference for Amanda French

Dear Sir / Madam,

Amanda worked for PDC Electronics in the operations department from 25th November 2005 until 27th May 2006 at which point she decided to leave in order to progress her career with another organisation.

During her time with us, Amanda was reliable and hard working. She had no unauthorised days off during her time with us and I have no evidence to suggest that she would be anything other than a benefit to your organisation.

Yours faithfully

Paula D. Corso – Managing Director

LDCC Basic Check Screening Form – D36 – Issue 2

This basic check screening form must be completed for all individuals who apply for a role at LDCC. All information provided will be verified by a human resources advisor on your first day of work should your application be successful. Please note that you will be required to bring ***original documents*** with you on your first day for this verification to be completed. Photocopies of documents will not be accepted.

Acceptable forms of identification for a British national are as follows:

Full 10 Year Passport

Driving license

Birth Certificate (issued within six weeks of birth)

Cheque book and bank card with three accompanying statements and proof of signature

Credit card with photograph

Utility bills (electricity, telephone, gas, water)

Council tax bill.

Please note that the following are NOT ACCEPTED as proof of identification:

International driving licenses

Copy of birth certificate issued more than six weeks after birth

Forces ID card

Library card

National Insurance number

Mobile telephone bill

Marriage certificate

Provisional driving license

IDENTITY CHECK Please confirm the following information:	
Your Full Name	Graham Spring
Your Full Address	46 Goring Way Greenford

	Middlesex UB6 8JB
Your Nationality	British
Your Marital Status	Single
REFERENCES	
Please provide the name and address of at least two referees, one of which should be your most recent employer.	
REFERENCE 1	
Name:	John Schofield
Address:	Uxbridge Technical College 15 George Street Uxbridge Middlesex UB2 4TT
Telephone Number:	0208 230 2300
Relationship to you:	Course Tutor
REFERENCE 2	
Name:	Steven Pearson
Address:	The Manse 50 Church Lane Greenford Middlesex UB6 3WS
Telephone Number:	0208 487 7968
Relationship to you:	Church Minister
Please provide details of your education and any relevant professional qualifications.	7 GCSEs from Uxbridge High School Diploma in Computing from Uxbridge Technical College

CRIMINAL RECORDS DECLARATION (Complete only one section)

I HAVE NO CONVICTIONS, WHETHER SPENT OR UNSPENT, CAUTIONS, REPRIMANDS, OR FINAL WARNINGS.

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature ………Graham Spring……………………………………….(Applicant) Date 12/12/10

I HAVE THE FOLLOWING CONVICTIONS, CAUTIONS, REPRIMANDS AND/OR FINAL WARNINGS:

(record below details of any and all convictions, whether spent or unspent, cautions, reprimands and / or final warnings that you may have to declare)

………

………

………

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature……………………………………………… (Applicant) Date …./……/……

Please note that all employees should expect to undertake Government standard security clearance. If you believe you will not be able to attain such clearance then please indicate below the reason for this.

I believe I may not be able to attain Government standard security clearance because:

THE FOLLOWING SECTION IS TO BE COMPLETED BY HR	
EVIDENCE SEEN	DATE SEEN
IDENTIFICATION	
Full British Passport	18/01/11
Student Union Card	18/01/11
EDUCATION AND QUALIFICATIONS – CERTIFICATES SEEN (if any)	
Diploma in Computer Studies	15/12/10
REFERENCES	
Reference 1 Verified **YES** / NO (delete or highlight as applicable)	
Reference 2 Verified YES / **NO** (delete or highlight as applicable)	
If references were not able to be verified or were not available please enter details here regarding why this is the case:	
Checked by:	Signature:

LDCC

Technical College

To: Whomever it may concern

Subject: Reference for Graham Spring

Dear Sir / Madam,

In response to your request for a reference for Graham Spring.

I can confirm that Graham attended this college from September 2008 and left in June 2010. He studied computing and was awarded a Diploma in Computer Studies in July 2010.

Yours faithfully

John Schofield

Course Tutor

LDCC Basic Check Screening Form – D36 – Issue 2

This basic check screening form must be completed for all individuals who apply for a role at LDCC. All information provided will be verified by a human resources advisor on your first day of work should your application be successful. Please note that you will be required to bring ***original documents*** with you on your first day for this verification to be completed. Photocopies of documents will not be accepted.

Acceptable forms of identification for a British national are as follows:

Full 10 Year Passport

Driving license

Birth Certificate (issued within six weeks of birth)

Cheque book and bank card with three accompanying statements and proof of signature

Credit card with photograph

Utility bills (electricity, telephone, gas, water)

Council tax bill.

Please note that the following are NOT ACCEPTED as proof of identification:

International driving licenses

Copy of birth certificate issued more than six weeks after birth

Forces ID card

Library card

National Insurance number

Mobile telephone bill

Marriage certificate

Provisional driving license

IDENTITY CHECK Please confirm the following information:	
Your Full Name	Yan Kypers
Your Full Address	45a Coopers Crescent Fulham

	London SW6 4SG
Your Nationality	South African
Your Marital Status	Married
REFERENCES	
Please provide the name and address of at least two referees, one of which should be your most recent employer.	
REFERENCE 1	
Name:	Tony Jones
Address:	Harwood Arms Walham Grove London SW6 1QP
Telephone Number:	020 7386 1847
Relationship to you:	Manager
REFERENCE 2	
Name:	Anton Kruup
Address:	Rainbow Insurance plc Ojo Adeyinka Way Sandton Johannesburg South Africa
Telephone Number:	+27 860 054 321
Relationship to you:	Team Leader
Please provide details of your education and any relevant professional qualifications.	10 Higher certificate passes (S. Affica) 3 Advanced level passes (Africa)
CRIMINAL RECORDS DECLARATION (Complete only one section)	

I HAVE NO CONVICTIONS, WHETHER SPENT OR UNSPENT, CAUTIONS, REPRIMANDS, OR FINAL WARNINGS.

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature ………Yan Kypers……………………………………….(Applicant) Date 10/08/12

I HAVE THE FOLLOWING CONVICTIONS, CAUTIONS, REPRIMANDS AND/OR FINAL WARNINGS:

(record below details of any and all convictions, whether spent or unspent, cautions, reprimands and / or final warnings that you may have to declare)

………

………

………

As the applicant for the position I confirm that the details shown above are an accurate record of any criminal offences that may appear on my Criminal Records Disclosure and understand this will be discussed if I am invited to an interview.

Signature……………………………………………… (Applicant) Date …./……/……

Please note that all employees should expect to undertake Government standard security clearance. If you believe you will not be able to attain such clearance then please indicate below the reason for this.

I believe I may not be able to attain Government standard security clearance because:

…making excellence a habit.™

THE FOLLOWING SECTION IS TO BE COMPLETED BY HR	
EVIDENCE SEEN	DATE SEEN
IDENTIFICATION	
Full South Africa Passport	02/09/12
Electricity bill	02/09/12
Work Permit	02/09/12
EDUCATION AND QUALIFICATIONS – CERTIFICATES SEEN (if any)	
N/A	
REFERENCES	
Reference 1 Verified **YES** / NO (delete or highlight as applicable)	
Reference 2 Verified **YES** / NO (delete or highlight as applicable)	
If references were not able to be verified or were not available please enter details here regarding why this is the case:	
Reference is in S Africa, sent but reply not received, so requested another one - PHP Ltd	
Checked by:	Signature:

Harwood Arms
Walham Grove

To: Whomever it may concern

Subject: Reference for Yan Kypers

Dear Sir / Madam,

In response to your request for a reference for Yan Kypers

I can confirm that he was employed as a barman from March 2012 to August 2012.

His attendance record during his employment was very good and he was popular with our regular customers.

Yours faithfully

Tony Jones

Landlord

PHP Ltd

To: Whomever it may concern

Subject: Reference for Yan Kypers

Dear Sir / Madam,

In response to your request for a reference for Yan Kypers.

I can confirm that Yan was employed as a Senior Customer Services Administrator from March 2012 to April 2012.

It is the policy of this company to limit references to this information only as we unfortunately had to relieve him of his duties due to suspected theft.

Yours faithfully

Clare Jones

HR Administrator

Performance Monitoring and Measurement (Extract) - D37 - Issue 3

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
1	1. Adherence to the RTP implementation schedule	See Information Security Risk Treatment Plan - RTP A -17 Schedule.	Document review - Actions undertaken from the RTP will be delivered within plan timelines	Completed sections from the RTP A - 17 schedule	100%	Monthly
2	2. Verification records of backups are documented and retained (according to criteria)	See Information Security Risk Treatment Plan - RTP A -17	Document review - Backups taken against the backup procedure will be reviewed. Document review	Documents up to date and complete	100%	Monthly
3	3. 'Restoration' testing is carried out according to procedures	See Information Security Risk Treatment Plan - RTP A -17	As above	Evidence of restoration testing	100%	Monthly

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
4	4. Testing of 'Restoration': data is then available, with no loss of integrity	See Information Security Risk Treatment Plan - RTP A -17	As above	Evidence of 'successful' restoration.	100%	Monthly
5	1. Formal exchange agreements shall be created to protect the transfer of information through the use of all types of communication facilities.	See Information Security Risk Treatment Plan – RTP A1	Document Review - Existence of approved for use non disclosure agreement template	Approvals	Completed	As necessary
6	2. Formal exchange agreements shall be then implemented.	See Information Security Risk Treatment Plan – RTP A1	Document Review - Non disclosure agreements inplace for partners	Numbers returned	100% from partner list	As necessary

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
7	3. An appropriate policy & procedure shall be created to ensure exchange agreements are implemented.	See Information Security Risk Treatment Plan – RTP A1	Document Review - Existence of policy & procedure to structure the use of non disclosure agreements	Approved procedure	Completed	Once
8	1. Adherence to the RTP implementation schedule	See Information Security Risk Treatment Plan – RTP EI - 6 Schedule.	Document review - Actions undertaken from the RTP will be delivered within plan timelines	Broken or disabled locks, obstructions, missed upgrades	100% operational and closed as default, 100% implementation of planned actions	Monthly

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
9	2. Completion of locks and access system installation	Information Security Risk Treatment Plan – RTP EI - 6 Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. A program is underway to improve physical security.	Inspection - Walk around looking at systems that match invoices	Are locks and systems working, signed off	Completed	Once
10	3. Audit of adherence to 'card issuing' procedures (new starter card issuing requests being actioned and leavers being de-activated)	Information Security Risk Treatment Plan – RTP EI - 6 Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. A program is underway to improve physical security.	Document Review - The review of new starter and leaver HR documentation	Starters with the correct cards and leavers cards returned and logged	100%	Quarterly
11	4. Observation on the use of the system at peak entry times.	Information Security Risk Treatment Plan – RTP EI - 6 Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. A program is underway to improve physical security.	Observation - Watching the staff come and go.	Passes being used, doors closed	90%	Monthly

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
12	1. Procedures for pre-employment screening shall be developed and implemented in accordance with the RTP schedule	See Information Security Risk Treatment Plan – RTP II -11 Schedule.	Document Review - Existence of approved procedure for screening	Missed staff, incomplete records	100%	Once
13	2. Screening for all new employees to start no later than three months from the commencement of the project	Information Security Risk Treatment Plan – RTP II -11 Background verification checks on all candidates for employment.	Document Review - Existence of screening evidence	Complete HR records within timeline	100%	Once
14	3. Completed HR records for screened employees to be available for inspection upon commencement of employment	Information Security Risk Treatment Plan – RTP II -11 Background verification checks on all candidates for employment.	Document Review - Existence of screening evidence	Complete HR records	100%	Quarterly

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
15	OBJ A2 LDCC Customer contact Information	Completion schedule 1. 1 month after permanent sales director appointed 2. As and when this is needed	Document Review - Existence of evidence	Completion to schedule	100%	Quarterly
16	OBJ EI - 2 Hacking and Unauthorized Interception	Completion schedule 1. Implementation Resource Estimates The following rough-order-magnitude timeframes represent the calendar time required by staff / supplier to implement each of the practices described in the ‘Proposed Actions section’. 1. Design the firewall system 3 months 2. Acquire firewall hardware and software 2 months 3. Acquire firewall documentation, training, and support 1 month 4. Install firewall hardware and software 1 month 5. Configure IP routing 1 week 6. Configure firewall packet filtering 3 weeks 7. Configure firewall logging and alert mechanisms 2 weeks 8. Test the firewall system 2 weeks 9. Install the firewall system 1 week 10. Phase the firewall/IP system into operation 2-3 months	Document Review - Existence of evidence	Completion to schedule	100%	Quarterly

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
17	OBJ EI - 5 Technology Expectations	Completion schedule 1. 1 month 2. 2 weeks after 1 3. 1 month after 2 4. 1 month after 3 4. After 4	Document Review - Existence of evidence	Completion to schedule	100%	Monthly
18	Legal	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Document Review - Existence of evidence	Missed items, knowledge of staff and awareness of information sources	Up-to-date, Knowledge of future and recent changes	Annual
19	Resources	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Document Review - Existence of evidence	Up to date, match expectations, understandable	Output valuable in predicting future needs	6 Monthly
20	Physical Protection	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Inspection - Walk around looking at desks	Files, printing , Post IT notes	0%	Monthly

No	Process / Control / Other	Description	Methods	Key Indicator(s)	Measurement acceptance target	Review Frequency
21	Passwords	Password management systems shall be interactive and shall ensure quality passwords.	Document Review - Existence of evidence	Strong password requirements working on new accounts and changed passwords	100%	Annual
22	Media shall be protected from unauthorised access	Media shall be protected from unauthorised access	Inspection - Walk around looking at media	Actual names recorded against approved access list	100%	Monthly

Performance Analysis and Evaluation (Extract) - D38 - Issue 2

No	Process / Control / Description	Date Last Analysed / Evaluated	Most recent Status	Previous date 1	Previous date 2	Previous date 3	Target % Achieved	Who Analyzed & Reviewed	Conclusion
1	1. Adherence to the RTP implementation schedule	19/10/xx	Completed	22/09/xx	22/08/xx	20/07/xx	100%	The Management Information Security Forum (ISF)	Excellent
2	2. Verification records of backups are documented and retained (according to criteria)	20/10/xx	Completed	20/09/xx	22/08/xx	NA	100%		Excellent
3	3. ‘Restoration’ testing is carried out according to procedures	20/10/xx	Some failures are evident still	20/09/xx	22/08/xx	NA	100%		We need to find out why this is still happening

No	Process / Control / Description	Date Last Analysed / Evaluated	Most recent Status	Previous date 1	Previous date 2	Previous date 3	Target % Achieved	Who Analyzed & Reviewed	Conclusion
4	4. Testing of 'Restoration': data is then available, with no loss of integrity	20/10/xx	Loss of data is evident still	20/09/xx	22/08/xx	NA	100%		We need to find out why this is still happening
5	1. Formal exchange agreements shall be created to protect the transfer of information through the use of all types of communication facilities.	20/09/xx	Completed	NA	NA	NA	100%		Excellent
6	2. Formal exchange agreements shall be then implemented.	19/11/xx	Completed	NA	NA	NA	100%		Completed before schedule - good work

No	Process / Control / Description	Date Last Analysed / Evaluated	Most recent Status	Previous date 1	Previous date 2	Previous date 3	Target % Achieved	Who Analyzed & Reviewed	Conclusion
7	3. An appropriate policy & procedure shall be created to ensure exchange agreements are implemented.	Due in April next year	Pending	NA	NA	NA	0%		Pending, but has it started yet as the above was finished early?
8	1. Adherence to the RTP implementation schedule	27/10/xx	In progress	25/09/xx	24/08/xx	23/07/xx	100%		Excellent
9	2. Completion of locks and access system installation	19/10/xx	In progress	25/09/xx	24/08/xx	23/07/xx	100%		Excellent
10	3. Audit of adherence to ‘card issuing’ procedures (new starter card issuing requests being actioned and leavers being de-activated)	19/11/xx	Completed	NA	NA	NA	100%		Need to gather audit results for the ISF Review - no date at last review?

No	Process / Control / Description	Date Last Analysed / Evaluated	Most recent Status	Previous date 1	Previous date 2	Previous date 3	Target % Achieved	Who Analyzed & Reviewed	Conclusion
11	4. Observation on the use of the system at peak entry times.	19/11/xx	Completed	NA	NA	NA	100%		As above!
12	1. Procedures for pre-employment screening shall be developed and implemented in accordance with the RTP schedule	22/06/xx	Completed	NA	NA	NA	100%		Excellent
13	2. Screening for all new employees to start no later than three months from the commencement of the project	22/07/xx	Completed	NA	NA	NA	100%		Excellent

No	Process / Control / Description	Date Last Analysed / Evaluated	Most recent Status	Previous date 1	Previous date 2	Previous date 3	Target % Achieved	Who Analyzed & Reviewed	Conclusion
14	3. Completed HR records for screened employees to be available for inspection upon commencement of employment	22/08/xx	Completed	NA	NA	NA	100%		HR have informed the ISF that the latest completed records cannot be located - suspected lost. They will however send to the ISF previous records on file. *(Received - Excellent)*
15	OBJ A2 LDCC Customer contact Information	17/11/xx	Pending	N/A	NA	24/08/xx	100%		Still no permanent Sales Director appointed - NO PROGRESS!
16	OBJ EI - 2 Hacking and Unauthorized Interception	01/10/xx	Pending	01/07/xx	01/04/xx	NA	100%		Resources still not provided - Budget not approved (cash flow issues still). Told to make the best of what we have for now
17	OBJ EI - 5 Technology Expectations	01/11/xx	Pending	01/10/xx	NA	NA	100%		Told that resources will be an issue as per the above. The ISF are not happy with Top Management commitment to IS
18	Legal	30/06/xx	?	Last year	NA	NA	100%		No point in reviewing the below until resources are budgeted for (don't want the same issues as the above).
19	Resources	17/11/xx	?	17/02/xx	NA	NA	100%		No comment

No	Process / Control / Description	Date Last Analysed / Evaluated	Most recent Status	Previous date 1	Previous date 2	Previous date 3	Target % Achieved	Who Analyzed & Reviewed	Conclusion
20	Physical Protection	01/11/xx	?	01/10/xx	01/09/xx	01/08/xx	100%		No comment
21	Passwords	12/04/xx	?	Last year	NA	NA	100%		No comment
22	Media Protection	09/11/xx	?	09/10/xx	09/09/xx	09/08/xx	100%		No comment

Continual Improvement

Internal Audit Programme (201x) *[Extract]* - D39 – Issue 1

	Mar	April	May	June	July	Aug	Sept	Oct	**Nov**	Dec	Jan	Feb
Reporting of IS Events				**X**								
Physical Access Control		**X**			**X**			**X**				
Ownership of Assets			**X**				**X**					
Clear Desk and Clear Screen				**X**								
Password Use	**X**		/		**X**		**X**		**X**			
Information Backup				**X**		**X**						
Network Routing Control												
Corrective Action				**X**				**X**				
Resource Screening									**X**			
Network access controls		**X**			**X**			**X**				
Risk Assessment Procedures	**X**		**X**		/		**X**		/			
Temporary Passwords				**X**		**X**						

Internal Audit Report – D40 – Issue 1

Internal Audit Report	
Auditor: Gordon Black	**Auditee: John Bishop**
Audit Objective: To assess the implementation & effectiveness of Procedure ‘Ownership of Assets’ Version 3 11/01/20xx	**Date: 17/09/2013**
Audit Scope: All areas and activities covered within the Information Security Control – Ownership of Assets	**Audit Criteria: ISO 27001 Controls Covered: A7.1.2 & ‘Ownership of Assets’ Version 3 11/01/20xx Procedure**

Audit Summary & Findings:

An asset register exists which is documented to contain the records of all organisation assets. The auditee was able to demonstrate the existence of this register.

Evidence: LDCC Asset Register – version 1.2

Within the register, asset LDCC-C-17 (a user computer) was identified for review. The auditee demonstrated that the asset had a complete record of who owns the asset, the asset location, when it was last built and when it was last accounted for. The auditee called the owner who verified their ownership of the record.

On further review of other assets, it was identified that a number of assets didn’t contain complete records of information.

- LDCC-S-11 (a network switch) had no documented owner
- LDCC-L-02 (a user laptop) showed a recorded build date of 2+ years ago and has no known location or evidence of use on LDCC systems
-

Minor N/C: Identified assets (above) do not contain complete information records which the auditee couldn’t explain or demonstrate.

Internal Audit Report – D40 – Issue 1

Internal Audit Report	
Auditor: Fay Woodward	**Auditee: Joe Cullum, Lucy Carr, Lauren Hunter, Tracey Baker and Colin Strange.**
Audit Objective: ISO 27001 Clauses and Controls Covered: 11.3.1	**Date: 17/09/2013**
Audit Scope: Information Security Control – Password Use	**Audit Criteria: LDCC**

Audit Summary & Findings:

Generally, it is observed that passwords are being used in line with the relevant policies. Users are aware of the need for password complexity (based on their staff awareness training) and observe the control required over their personal levels of access to systems.

Staff were very courteous to me as I’ve never inspected this area before, so help was provided in raising the N/C’s (required by the IS Manager) below.

Evidence:

Minor N/C 1: One of the auditees had a password written down in their day book which was left in plain view on her desk
Minor N/C 2: One of the auditees could not identify any of the minimum password requirements or where to find them

NONCONFORMITY/CORRECTIVE ACTION FORM – D41 – Issue 1

DATE: 19/09/20XX	DATE LOGGED: 20/09/20XX

2. DEPARTMENT/ LOCATION: Gordon Black / Internal Audit Ownership of Assets

3. NONCONFORMITY OR ACTION REQUEST:

Actual Problem identified (completed by originator)

A number of assets didn't contain complete information records which the auditee couldn't explain or demonstrate a valid record of:

- LDCC-S-11 (a network switch) had no documented owner
- LDCC-L-02 (a user laptop) showed a recorded build date of 2+ years ago and has no known location or evidence of use on LDCC systems

Possible solution (completed by originator)

Identify the incomplete data and update master records accordingly.

4. LINE MANAGER/PROCESS OWNER ASSIGNED: John Bishop (Team Leader/IT Manager)	DATE DUE: Within a week

5. DETAILS OF ACTUAL CORRECTIVE ACTION (completed by assignee):

As suggested above. Took much longer than thought as we uncovered lots of unusual assets not accounted for in the Asset Register.

SIGNED: John Bishop (IT Manager)	DATED: 08/11/20XX

6. ORIGINATORS ACCEPTANCE: The new asset register should be submitted to the next ISF for review and a follow up audit arranged next month.

SIGNED: Gordon Black (ISMS Auditor)	DATED: 08/11/20XX
	Acceptable/Not Acceptable (If unacceptable re-raise CAR/PAR)

7. INCLUSION IN AUDIT PROGRAMME **YES**/NO

NONCONFORMITY/CORRECTIVE ACTION FORM – D41 – Issue 1

DATE: 17/09/20XX	DATE LOGGED: 19/09/20XX

2. DEPARTMENT/ LOCATION: Fay Woodward Internal Audit – Password Use

3. NONCONFORMITY OR ACTION REQUEST:

Actual Problem identified (completed by originator)

Minor N/C 1: One of the auditees had a password written down in their day book which was left in plain view on her desk

Minor N/C 2: One of the auditees could not identify any of the minimum password requirements or where to find them

Possible solution (completed by originator)

N/C 1 Issue refresher of staff awareness with emphasis on our password policy and the control of user passwords. Review the effectiveness of IS Induction Training with other members of staff – is this a one off?

N/C 2 Issue a bulletin identifying the location for the ISMS policy and where users can find password requirements for LDCC. Recheck with other staff in a month's time to assess if staff can now identify password requirements and where to find them.

4. LINE MANAGER/PROCESS OWNER ASSIGNED: Clive Prichard (IS Manager)	DATE DUE: Within 2 weeks

5. DETAILS OF ACTUAL CORRECTIVE ACTION (completed by assignee):

N/C 1 This has been scheduled for review with the ISF (effectiveness assessment) ahead of instigating a new staff awareness training session. In the interim, I have sat with the auditee and provided an overview of the password policy as well as the key sections from IS policy with regard to user controls. Next ISF is scheduled for 21/09/XX

N/C 2 This has been created and sent for review with the ISF ahead of publishing to the intranet. In the interim, I have sat with the other auditee and provided an overview of the password policy. Will re-check after one month as above.

SIGNED: Clive Prichard (IS Manager)	DATED: 26/09/20XX

6. ORIGINATORS ACCEPTANCE: Thanks.	
SIGNED: *Fay Woodward* (Auditor)	DATED: 27/09/20XX
	Acceptable/Not Acceptable (If unacceptable re-raise CAR/PAR)

7. INCLUSION IN AUDIT PROGRAMME YES/**NO**

Incident Log – D42 – Issue 3

Event (possible breach)/Incident (IS threat) Log (Extract)

Individual Event Reports provide the detail and help determine an IS threat. The information security manager is required to review all IS Events raised and then decide if an IS Incident has occurred. A Nonconformity report (for any information security incidents) is then to be raised, as appropriate.

Ref	IS Event Description	Reported by	Date	IS Incident?	Incident Owner	Status	Close Date
IL1	Loss of USB Stick	Graham Spring	11/5/20XX	No	N/A	N/A	N/A
IL2	Virus on Laptop	Martin Pearson	2/6/20XX	Yes	John Bishop	Closed	10/6/XX
IL3	Power Failure	Geoff King	6/6/20XX	No	N/A	N/A	N/A
IL4	Sales Director’s Laptop Stolen	Clive Page	20/6/20XX	Yes	Clive Prichard	Closed	23/6/XX
IL5	Misuse of Internet	Fay Woodward	8/7/20XX	No	N/A	N/A	N/A
IL6	Loss of USB stick	Tracey Baker	2/8/20XX	No	N/A	N/A	N/A
IL7	Confidential papers in standard waste bins	Philip Hernshaw Smyth	15/8/20XX	Yes	N/A	N/A	N/A
IL8	Loss connectivity to the Internet	Lucy Carr	27/8/20XX	No	N/A	N/A	N/A
IL9	Client activity reports found on printer	Fay Woodward	22/9/20XX	Yes	Lucy Carr	Closed	23/9/20XX
IL10	Unauthorized software discovered on network	Colin Strange	23/9/20XX	Yes	Lauren Hunter	In Progress	
IL11	Power failure	Geoff King	16/10/20XX	No	N/A	N/A	N/A
IL12	Unknown visitor found in Main IT Room	Sarah Wallmarsh	14/11/20XX	No	N/A	N/A	N/A

NONCONFORMITY/CORRECTIVE ACTION FORM – D41 – Issue 1

DATE: 22/09/20XX	DATE LOGGED: 23/09/20XX

2. DEPARTMENT/ LOCATION: Fay Woodward IL9 / Sales Department

3. NONCONFORMITY OR ACTION REQUEST:

Actual Problem identified (completed by originator)

Client activity reports found on printer.

Possible solution (completed by originator)

I would suggest to remove promptly and shred.

4. LINE MANAGER/PROCESS OWNER ASSIGNED: Lucy Carr (Tele Manager)	DATE DUE: Immediate.

5. DETAILS OF ACTUAL CORRECTIVE ACTION (completed by assignee):

Agreed actions (as above), but I was not informed till the day after, by that time there were no reports on the printer and the bin (next to the printer) had already been emptied by the cleaners. Anyway the nonconformity is no more as there are no reports on the printer.

SIGNED: Lucy Carr (Tele Manager)	DATED: 23/09/20XX
6. ORIGINATORS ACCEPTANCE: Sounds good to me.	
SIGNED: *Fay Woodward*	DATED: 23/09/20XX
	Acceptable/Not Acceptable (If unacceptable re-raise CAR/PAR)

7. INCLUSION IN AUDIT PROGRAMME YES/**NO**

NONCONFORMITY/CORRECTIVE ACTION FORM – D41 – Issue 1

DATE: 23/09/20XX	DATE LOGGED: 23/09/20XX

2. DEPARTMENT/ LOCATION: Colin Strange IL10 / IT Department

3. NONCONFORMITY OR ACTION REQUEST:

Actual Problem identified (completed by originator)

Unauthorized software discovered on network.

Possible solution (completed by originator)

Receptionist to identify visitors who may have had access to network and who probably loaded the unauthorized software onto the network. When identified please call the Police to investigate the visitor’s legitimacy.

4. LINE MANAGER/PROCESS OWNER ASSIGNED: Lauren Hunter (Receptionist)	DATE DUE: Immediate please.

5. DETAILS OF ACTUAL CORRECTIVE ACTION (completed by assignee):

I’m not happy identifying suspected suspect as many are our customer’s, but I’ll do my best – it may take some time though.

SIGNED: Colin Strange (IT Analyst)	DATED: 23/09/20XX
6. ORIGINATORS ACCEPTANCE: Sounds good to me, anyway I haven’t the experience for investigations of this type.	
SIGNED:	DATED:
	Acceptable/Not Acceptable (If unacceptable re-raise CAR/PAR)

6. INCLUSION IN AUDIT PROGRAMME YES/NO