Link Group

For all wholly owned subsidiaries within the Link Group

Information Classification and Handling Policy

Owner	Chief Information Security Officer, Link Group
Department:	Information Security, Technology & Innovation, Link Group
Document Name:	Information Classification and Handling Policy
Version Number:	2.6 as at 28/12/2018
Approved by:	Information Security Management Forum
Next Review Date:	December 2019

Table of Contents

1. Change Control Information

Version	Changed by	Date	Change Information
0.1	Dave Cowan	28/10/2013	First draft
1.0	Dave Cowan	28/10/2013	Released
2.0	Dave Cowan	04/12/2014	Annual Review
2.1	Dave Cowan	28/07/2015	Removed complexity in the policy
2.2	Dave Cowan	29/12/2015	Annual Review
2.3	Lance Torrance	29/12/2016	Annual Review
2.4	Lance Torrance	29/12/2017	Annual Review, update CTISO title.
2.5	Phil Ravenscroft, Lance Torrance, Anthony Handwerker	14/09/2018	Reduced to 3 levels of classification, updated the examples & updated 6.2 Personal Responsibilities.
2.6	Lance Torrance	28/12/2018	Annual Review, update CISO title, updated section 4 to clarify handling of data not yet classified.

2. INFORMATION CLASSIFICATION AND HANDLING

2.1 INTRODUCTION

Information is the critical asset that makes Link Group's business operations and client management possible.

In order to preserve information confidentiality, integrity and availability, users of the information need to understand how important each asset is and to apply the appropriate handling instructions.

This document explains:

- How to evaluate and assign an information classification;
- Which types of information belong in each classification band;
- The handling instructions associated with each classification type.

Like most organisations, Link Group is entirely dependent on the accuracy and availability of multiple information sets to develop, to provide and bill for services, to collect revenue and to meet regulatory and legislative obligations. The unintended loss, exposure or unauthorised change to any of the many sensitive Link Group information assets could have an extremely damaging effect on the company's ability to operate and could lead to substantial financial loss, legal repercussions, reputational damage and/or a fall in market value.

In order to minimise the risk of unintentional exposure of Link Group organisational data, it is critical to ensure that:

- Each Information set has an identifiable owner;
- The owner of each information asset classifies and labels it appropriately;
- Once suitably labelled, subsequent handling decisions made by users and system owners are guided by the instructions set out in this document.

This document sets out the process for criticality assignment, the handling rules for each classification of Information and the associated roles and responsibilities.

2.2 SCOPE

This Policy is applicable to all Link Group employees, contractors and third party personnel with access to Link Group information and/or systems.

This Policy shall apply to all information held or available in hard copy and/or electronic format, including but not limited to MS Office documents, email, the contents of databases and computer source code.

An “Information set” is a collection of Information connected either by its subject matter or context. Example Information sets would include:

- A series of client related documentation;
- Information processed within an application;
- The contents of a database;
- A group of network diagrams;
- Letters posted to a member of the Board;
- System management traffic;
- Customer complaints.

This policy supports the Link Group Information Security Policy and IT Security Policy.

3. ROLES & RESPONSIBILITIES

3.1 C-SUITE AND/OR HEAD OF DEPARTMENT

The C-suite and/or each Head of Department must ensure that:

- A named owner is assigned to all new information sets generated by a project, initiative or other activity;
- No assigned Information Owner is relieved of his/her accountabilities on changing roles without that accountability being reassigned to another named individual;
- The Link Group Asset Classification Register is populated as described in this Policy;
- The Asset Classification Register is subject to regular review and updating;
- A process for the classification of legacy information sets is introduced and managed;
- The requirements defined in this Policy are met or the risk acceptance is signed off and recorded by the Chief Information Security Officer as an exception to the Policy.

3.2 BUSINESS OWNER (BUSINESS USER OF THE DATA)

The Business Owner must ensure that:

- A risk assessment is performed against the criteria laid out in this Policy and an appropriate classification assigned;
- Enterprise application related information is labelled with the assigned classification and entered onto the Asset Classification Register (see form in Appendix A);
- Privileged and Confidential information is assigned a classification expiry date and reviewed for currency on or before that date;
- End user generated information is labelled with the assigned classification;
- Application Owners/Asset Custodians with responsibility for solutions design and/or operations of systems processing the information are made aware of the classification;
- Any gap shortfall between the Asset Custodians proposed security solution and the handling requirements defined in this Policy is considered and challenged, as deemed appropriate;
- Any instance of that shortfall and the associated risk acceptance is referred to the Chief Information Security Officer as an Exception Request (see form in Appendix B);

- All information sets classified as Confidential and above are subject to review no less frequently than once a year.

3.3 APPLICATION OWNER/ASSET CUSTODIAN (PERSON RESPONSIBLE FOR DESIGN/ACCESS REVIEW/MAINTENANCE)

The Asset Custodian must ensure that:

- The information classification is considered as part of the solutions design process;
- Solutions meet the security requirements defined in this document;
- The security solution is clearly documented and includes an end-to-end security schematic as illustrated in the Link Group Security Architecture Standard;
- Any proposed shortfall between the solution design and this Policy are clearly documented;
- Owners of underlying platforms and databases are aware of the security requirements;
- The security solution is end-to-end and accounts for every level including application, operating system, database and network;
- Where a shortfall seems appropriate, there is timely liaison with the Chief Information Security Officer before finalising the proposed design.

3.4 USERS

Users must ensure that:

- The handling instructions defined in this Policy are diligently followed.

3.5 CHIEF INFORMATION SECURITY OFFICER

The Chief Information Security Officer must ensure that:

- The Asset Classification Register is populated, managed and maintained;
- Exception Requests submitted by Business Owners or Asset Custodians are considered in a timely manner;
- Where an Exception Request is deemed appropriate, either a time-bound waiver or a complete dispensation is issued and recorded in the Risk Register;
- Where an Exception is not believed to be appropriate and liaison with the Information and Business Owners/Asset Custodians cannot reach a resolution, a Risk Assessment is documented and made available to senior management for a decision to be made.

4. INFORMATION CLASSIFICATION CATEGORIES

There are three information classification categories for Link Group data. The following matrix describes each classification type and gives examples of each:

In the absence of any classification, all information is to be classified as **PUBLIC** and handled accordingly.

However, in instances where a document or dataset has not yet been formally classified and labelled and a reasonable person would classify the document or dataset as containing data of a restricted or sensitive nature, then the document or dataset is to be taken to have a 'Confidential' classification and handled accordingly until formally classified and labelled.

Classification	**Description**	**Examples**
Privileged	Price sensitive information or information which the unauthorised disclosure of would lead to loss of competitive advantage and access to which should be restricted to named individuals (or post holders).	Negotiations concerning mergers and acquisitions. Profit forecasts. Board Minutes. Unpublished results. Bid documents or contracts.
Confidential	Impact of exposure, loss, unintended change or misuse has the potential to generate: • Losses greater than $10k AUD • Prosecution or other legal action • Negative media attention • Multiple faults or failures Information that provides insight into or definition of company processes, structures, planning, organisation, tactics or strategy and that could provide a competitor with an advantage. This classification label should also be used for documents within a closed community such as directors, HR, Finance, Internal Audit etc.	Third Party information subject to confidentiality obligations. Personal Information as defined by regulation (e.g. Privacy Act. 1988, General Data Protection Regulation 2018). Supplier selection related data. Billing Systems. Email systems. Archiving systems. Budgetary forecasts, planning or results. Network diagrams. Operational processes. Project and planning information. Source code Information related to Security Incidents, Security Risks or Security Controls; GS007 reports or other audit reports.

		Communications with regulators, auditors and consultants. Policies, procedures or guidelines not intended for the general public. Link Group financial or operational business documentation e.g. financial statements or insurance, policies, procedures, processes, standards, etc.
Public (Unrestricted)	All other information, which is non-sensitive or unrestricted and where exposure would have no impact or where disclosure and access are required by law. Eg. Privacy Policy, ASX announcements etc. Contains non-classified information which can be shared freely with anyone. If the information is not labelled it is therefore deemed to be Public.	Public web site data. Published customer service summary performance figures. Policies and procedures deemed to be in the public interest.

5. INFORMATION CLASSIFICATION METHODOLOGY

5.1 INFORMATION OWNERSHIP

At the point of creation, or as soon as possible thereafter, all information sets must be evaluated against the classification definitions, assigned a classification and labelled appropriately. All information sets, even those that are Public (unclassified), must be assigned a named owner, ideally the Head of the Department with the business requirement to generate or process that data, i.e. the individual who best understands the nature of the information and the likely impact of exposure or loss.

Where a system plays a key part in the business operations of more than one business area, it may be necessary to assign a panel of Asset Custodians, acting in concert under the leadership of primary Business Owner agreed by them all.

The named Business Owner is accountable for the classification of the information and for ensuring that the facilities or capabilities exist to enable appropriate handling. Once the information has been classified, labelled and the Business Owner has confirmed that there are no circumstances that would prevent an ordinary user from handling the information as instructed, the responsibility for ensuring handling instructions are followed falls to the user.

Business Owners must review their information sets on an annual basis to ensure that they remain current and that no changes have occurred that would impact classification or handling. The review must be recorded in the Asset Classification Register via the Chief Information Security Officer.

Incidents of information mishandling i.e. any failure to follow the instructions set out in this Policy will be reported to the Chief Information Security Officer, investigated and, where the risk is deemed to have been significant, reported to the RMAC.

5.2 CLASSIFICATION PROCESS

The Business Owners must evaluate the sensitivity of an information set by comparing it with the descriptions and examples provided in the matrix and considering the following questions:

- What would be the worst-case impact if this information became public?
- What would be the worst-case impact if this information were irretrievably lost?
- What would be the worst-case impact if this information were subject to unknown and unauthorised change?

Business Owners must consider each information set's criticality not only in isolation, but also in the context of the wider Link Group information estate. An information set assessed in isolation may be of little or no importance, but if associated with another information set, its level of sensitivity may increase by a large factor.

Information classified as Privileged or Confidential must be assigned a classification expiry date (review date) at which point the Business Owner must review its purpose, classification and applied controls. If all of the criteria remain current and appropriate, the Business Owner must re-validate the classification, assign a new classification expiry date and inform the Chief Information Security Officer so that the Asset Classification Register can be updated.

In the instance where a document or dataset has not yet been formally classified and labelled and a reasonable person would classify the document or dataset as containing data of a restricted or sensitive nature, then the document or dataset is to be taken to have a 'Confidential' classification and handled accordingly until formally classified and labelled.

The Business Owner has primary responsibility for the assignment and continuous maintenance of information classification. However, the Chief Information Security Officer will proactively encourage Business Owners to fulfil their obligations and, where there appears to be inconsistency in an evaluation, the Chief Information Security Officer may seek justification for a decision. Where there is uncertainty, the final risk decision lies with the C-suite executive of the associated business area.

5.3 REGISTRATION OF INFORMATION LEADING TO ASSETS

Link Group maintains a register of all applications/systems/services and the information relating to each.

Each business area of Link Group must perform an evaluation of each application/system/service upon which it relies and its associated information and assign an owner and a classification. This information must then be added to the Link Group Asset Classification Register. (See Registration form in Appendix A).

The Chief Information Security Officer must manage and maintain the Link Group Asset Classification Register to ensure that:

- All applications have been assigned a Business Owner and classified;
- All applications have been assigned an Asset Custodian;

- Classification is consistent between applications/systems/services;
- The Asset Classification Register is accurate and current.

The Asset Classification Register must capture and record the following information for all applications and related information sets:

- Asset Identifier;
- Business Owner (Asset Owner) – and deputies, where applicable;
- Asset Custodian;
- Threat and Vulnerability
- Information Classification – CIA Model;
- Description of the existing controls (particularly specifying if it is personal information – not required for Privileged data);
- Control Adequacy;
- Asset Sensitivity;
- Expiry date of classification of Privileged and Confidential data;
- Retention Period;
- Estimated Financial Impact.

The Business Owner must assign a classification, ensure that it is recorded in the Asset Classification Register and communicate the classification to the associated Asset Custodians (i.e. operational management of applications and underlying Operating Systems and Databases).

Although only Asset Custodians are capable of implementing prescribed controls, it is possible to include selected controls in more than one layer of the associated system (i.e. at application and/or Operating System level). Therefore, the Business Owner must ensure that the method for delivering all required controls has been documented either in Project Design documentation or in another dedicated security document.

The Chief Information Security Officer will review project-related and other security design documents as they are created to ensure that requirements are being met and/or required exceptions are appropriately documented and reviewed.

5.4 END USER OWNED INFORMATION ASSETS

Information created by an end user is potentially just as valuable and sensitive as that processed and stored by an application/system/service. For example, if a network engineer creates a network schematic of the Link Group Corporate Network, it should be classified as Confidential because of the impact it could have if it was misused. To this end, the creator or author of every information asset originating from the end user community must ensure that the same rules with respect to ownership, classification and handling are applied.

Typically, there is no requirement to register End User data. The registration of Privileged data, however, is at the discretion of the Business Owner. Where a Business Owner elects to ensure that the handling instructions being applied to one of his or her assets need to be included in the Chief Information Security Officer’s moderation and review process, the existence and location of the asset should be added to the Asset Classification Register. No description of Privileged information is required.

6. HANDLING INSTRUCTION

6.1 ALIGNING CLASSIFICATION TYPES WITH CONTROLS

The following matrix provides an overview of the controls needed for the range of classifications:

Classification	Objectives of the control set
Privileged	Individual controls are applied to each instance of information to provide a detailed, step-by-step audit trail and the highest level of assurance that unauthorised access is inhibited
Confidential	A full spectrum of Information Security controls are applied
Public	No specified controls are required

The following matrix sets out the detailed handling instructions that are required (where technically possible) for information sets of each classification type:

Required Processing					
Process	**Security Controls**		**Privileged**	**Confidential**	**Public**
Risk Assessment	1.0	Classified	X	X	X
	1.1	Labelled with the classification	X	X	
	1.2	Assigned an Owner	X	X	X
	1.3	Added to the Asset Classification Register (Application/System data)	X	X	
	1.4	Added to the Asset Classification Register (End User data)	X		
Access Control	2.0	Protected by defined network perimeter controls	X	X	
	2.1	Protected whilst traversing untrusted networks	X	X	
	2.2	Segregated from users and less secure networks	X	X	
	2.3	All users uniquely authenticated as defined in the Link Group IT Security Policy	X	X	
	2.4	All system management traffic secured	X	X	
	2.5	User credentials encrypted	X	X	
	2.6	Secure authentication of management traffic managed by dedicated operational security team	X	X	
	2.7	Time bound access control/ expiry	X		
Logging	3.0	Account creation/ modification/ deletion	X	X	
	3.1	Log on, success/fail	X	X	
	3.2	All user and system level activity, such that all transactions can be associated with an individual	X	X	
Information	4.0	Encryption in storage	X		

Required Processing					
Process	Security Controls		Privileged	Confidential	Public
Storage	4.1	Encryption in transit	X	X	
	4.2	Restricted access to archived data	X	X	
Monitoring	5.3	Network based Intrusion Detection System	X	X	
	5.4	Host based Intrusion Detection System	X	X	
	5.5	Audit rights on Third Party organisations accessing Link Group networks and systems	X	X	
	5.6	Audit rights on Third Party organisations processing Link Group information on non-Link Group site	X	X	
	5.7	Investigation of uncontrolled data	X	X	
Reproduction (E.g. photocopying and printing)	6.0	A list of named authorised recipients defined by Business Owner	X		
	6.1	Obtain the Business Owner's consent and circulate no further than the defined list of named authorised recipients	X		
	6.2	Number each copy and maintain log of distribution, expiry and retrieval	X		
	6.3	A list of authorised roles defined by Owner e.g. HR		X	
	6.4	Obtain the owner's consent and circulate no further than the defined list of authorised roles		X	
Faxing	7.0	Addressee present for reception		X	
	7.1	Prohibited	X		
Destruction	8.0	Secure disposal of documents via a dedicated sack/bin/container and destruction facility	X	X	
	8.1	Disposal of documents via a shredder			
	8.1	Obsolete hardware or other media to be wiped using software specified for the purpose by Information Security	X	X	
	8.2	Obsolete hardware to be securely disposed of by Information Security	X		
Disclosure to third parties	9.0	Owner's consent and non-disclosure agreement	X	X	
	9.1	Non-disclosure agreement	X		
Document labelling	10.0	Wherever possible, classification on each page of the document (End User)	X	X	
	10.1	Name of Business Owner on Title page and document history where they exist as part of the format (End User). For other document formats, ensure a label is placed in a logical, visible location	X	X	
	10.2	Name of Business Owner and classification stored in Asset Classification Register	X	X	

Required Processing					
Process	**Security Controls**		**Privileged**	**Confidential**	**Public**
Despatch	11.0	Courier transport only; double envelope, internal labelling and hand-to-hand exchange with signatories confirming each step of the transfer process	X		
	11.1	A double envelope, no external labelling, but labelled internally		X	
	11.2	A single envelope without any specific type of labelling			X
Granting access rights	12.0	Business Owner only	X	X	
	12.1	Head of Department	X		
Hard Copy document Audit trail	13.0	Locked in a safe or other secure location when in storage	X		
	13.1	Addressee, number of copies made, location, address, destruction, witnesses	X		
	13.2	Only required at the Business Owner’s discretion		X	

6.2 PERSONAL RESPONSIBILITIES

Information of any classification can be exposed without the physical loss of documentation or leakage of information being stored or transmitted. The most obvious manner in which information can be leaked is through verbal communications, whether on the telephone, in meetings or through indiscreet conversations in public places.

Wall charts, white boards, flip charts and hand-outs are all potential conduits for the leakage of sensitive information and all must be appropriately disposed of by their owners at the end of each meeting. The Chairperson of the meeting has responsibility for ensuring the meeting room has been cleared of residual information.

All personnel must consider confidentiality and take due care when discussing Link Group business matters with any party. No non-public company information is to be relayed to Third Parties without the authorisation of line management and, in particular, no statements or comments must be made to members of the press or media other than through the authorised company communications channels.

All personnel have a responsibility to keep Link Group information secure and confidential. The following requirements must be adhered to at all times:

- Computer screens must be locked when unattended even for a short time;

- In order to ensure backups are effective, all information classified as Confidential or Public must be saved to a network drive and information classified as Privileged should be saved to a secure drive with appropriate access rights;

  - Information should not be left on printers, photocopiers and fax machines for longer than is absolutely necessary;

  - Transportable media, such as laptops or USB memory sticks, must be kept physically secured at all times and, wherever Privileged or Confidential information is stored, it must be subject to encryption using a product or mechanism approved by the Chief Information Security Officer;

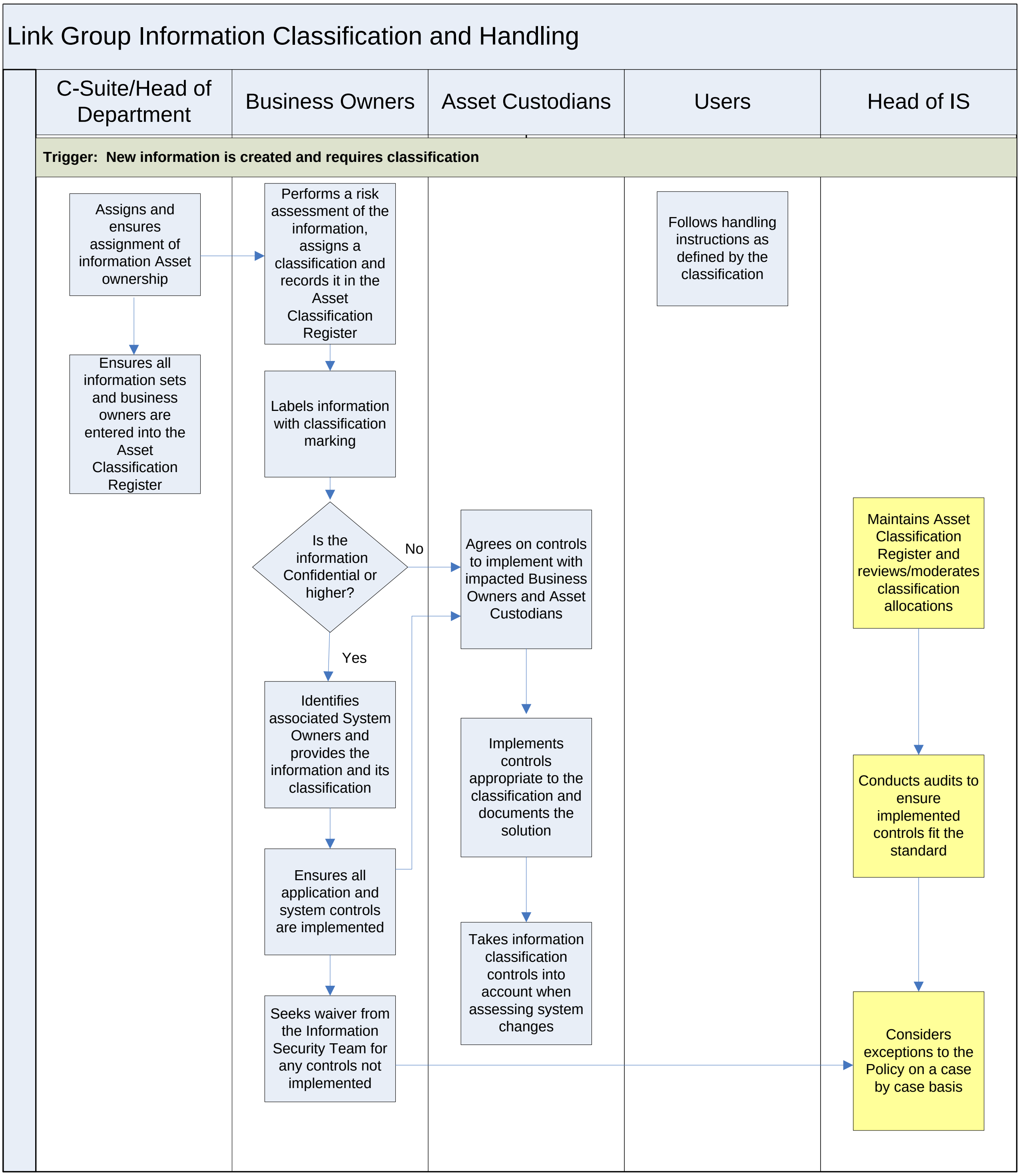
  - Privileged or Confidential files must not be stored in public folders; as the name suggests, such folders are public and so accessible by anyone with access to the Local Area Network;

  - The sender of a fax must obtain a print of the status of the transmission, which will confirm the number to which the fax has been sent or advise of a failed transmission and save the fax receipt in the appropriate network drive;

  - Cover sheets should be sent with all faxes advising the recipient to contact the sender if a fax is inadvertently sent to an unintended destination.

7. PROCESS

This Policy is implemented through the process below: see next page.



Link Group Information Classification and Handling

C-Suite/Head of Department

Business Owners

Asset Custodians

Users

Head of IS

Trigger: New information is created and requires classification

Assigns and ensures assignment of information Asset ownership

Ensures all information sets and business owners are entered into the Asset Classification Register

Performs a risk assessment of the information, assigns a classification and records it in the Asset Classification Register

Labels information with classification marking

Is the information Confidential or higher?

No

Yes

Identifies associated System Owners and provides the information and its classification

Ensures all application and system controls are implemented

Seeks waiver from the Information Security Team for any controls not implemented

Agrees on controls to implement with impacted Business Owners and Asset Custodians

Implements controls appropriate to the classification and documents the solution

Takes information classification controls into account when assessing system changes

Follows handling instructions as defined by the classification

Maintains Asset Classification Register and reviews/moderates classification allocations

Conducts audits to ensure implemented controls fit the standard

Considers exceptions to the Policy on a case by case basis

8. COMPLIANCE

The primary stakeholder concerned with the confidentiality, integrity and availability of a given set of information is the Business Owner. For this reason, with appropriate advice from solutions designers and the Chief Information Security Officer, any decision to accept risk associated with not implementing any of the controls defined in this Policy must be taken by the Business Owner. Having made the decision, irrespective of subsequent changes to roles and responsibilities, the Business Owner will continue to be held accountable for that decision for as long as he or she is in the employment of Link Group.

The Chief Information Security Officer will monitor and moderate the decisions made by Business Owners and work with Asset Custodians and the whole technology organisation to promote the availability of secure solutions in support of this Policy.

Where a risk accepted by an individual Business Owner is thought to have an implication for other systems, the Chief Information Security Officer will document a Risk Assessment and together with the Business Owner present the proposal and the risk to Senior Management for a decision.

Where the controls defined in this Policy are not met and no Exception Request is submitted to the Chief Information Security Officer for approval, the associated Business Owner may be subject to disciplinary action.