Information Security and Risk Management Policy

Policy Statement: This policy sets out standards for the management of information security and information risks across Telecoms Advisor Ltd

Revision History

Version	Status	Date	Consultee	Comments	Action from Comment
0.1	Draft	29/11/2017	MD		Decision to include

Table of Contents

Circulation

This policy applies to all staff who handle sensitive information across Telecoms Advisor Ltd. This includes staff responsible for:

1. introducing changes to services, processes or information
2. the management of information assets across Telecom Advisor Ltd.

This includes temporary and contract staff.

Scope

Includes

This policy outlines standards for information security and risk management across Telecom Advisor Ltd and covers the following areas:

- how to make a change to a current information asset
- the process to follow when developing a new information asset
- implementation of a new information asset
- information asset registration and review
- information asset retirement.

Definitions

Information is a corporate asset. Telecom Advisor Ltd's Information Assets are important sources of administrative and historical information. They are vital to Telecom Advisor Ltd to support its current and future operations (including meeting the requirements of the Freedom of Information legislation), for the purpose of accountability.

For the purpose of this policy **Information Assets (IAs)** are 'identifiable and definable assets owned or contracted by Telecom Advisor Ltd which are valuable to the business of the organisation'.

IAs will include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of data, and should not be seen as simply technical. Categories of IAs include:

- **Information:** Databases, system documents and procedures, archive media/data, paper records.
- **Software:** Application programs, systems, development tools and utilities.
- **Physical:** Infrastructure, equipment, furniture and accommodation used for data processing.
- **Services:** Computing and communications, heating, lighting, power, air-conditioning used for data processing.
- **People:** Their qualifications, skills and experience in the use of information systems.
- **Intangibles:** For example, public confidence in the organisation's ability to ensure confidentiality, integrity and availability of personal data.

The **Information Asset Register** documents information about all information assets across Telecom Advisor Ltd, and includes information about each asset owner (Information Asset Owner) and administrators (Information Asset Administrators).

Information Risk Management – A methodical information security risk assessment process which ensures that Telecom Advisor Ltd identifies, implements and manages controls to monitor and reduce the information security risks to the organisation, its person identifiable information and its critical information assets.

An **information risk** is the chance of something happening to information which is held by Telecom Advisor Ltd or their contractors, which will have an impact upon the organisations' business objectives. Information risks are measured in terms of *consequence* and *likelihood*, in accordance with the Risk Management Procedure.

Reason for Development

Information is only useful if it is correctly recorded in the first place, is regularly updated and is easily accessible when it

Aims and Objectives

The aim of this policy is to ensure that information security standards and processes are in place across Telecom Advisor Ltd.

Standards

Registering of information assets

An Information Asset Owner (IAO) or equivalent is assigned unique responsibility for each significant information asset, or group of assets at Telecom Advisor Ltd.

This IAO understands the scope and boundaries of their assigned information asset(s), their approved purposes, who the users of the assets are and what their requirements for guidance and training may be, the criticality of the assets to Telecom Advisor Ltd, their dependency on other assets, and which other assets are dependent on them.

All information assets held by Telecom Advisor Ltd should be registered on the Information Asset Register by the IAO.

The following categories of information about the asset are required for the registration process:

- Description
- Details of Information Asset Owner and Administrator and contact details
- Access Control Procedure
- Risk assessment of the asset (in accordance with the company Risk Management Policy)
- Business Continuity Plan
- Disaster Recovery Plan
- Operating Procedure.

The should record the information on a template attaching supporting documentation.

Information held on the Information Asset register will be reviewed on an annual basis.

Creation/Development and Implementation of Information Assets

Rapidly changing technology has an impact on processes and systems already in place, often requiring change simply to keep up to date and to enable the safe and secure processing of personal information.

It is therefore essential that all new or proposed changes to Telecom Advisor Ltd's processes and/or information assets, are identified and at an early stage.

Changes to an existing information asset should be documented. The request should be made by the existing IAO.

Proposed changes to an **organisational process** which might include the development of a new information system should be requested in the same way.

All implementations of new processes and information assets should follow a documented project management process.

Risk Assessment and Management

All critical information assets should be risk assessed annually (as a minimum) using Telecom Advisor Ltd Risk Assessment framework.

Each risk assessment should be clearly scoped and seek to identify, quantify and prioritise the information risks to Telecom Advisor Ltd's business functions. Consideration should also be given to information risks that may affect Telecom Advisor Ltd's business partners.

Risk Analysis

Risk analysis should be in accordance with Telecom Advisor Ltd's Risk Management Procedure, and should be completed on the Risk Management template.

Risk assessment steps should include as a minimum:

- location and source of risk;
- description of the risk;
- details of controls in place to manage risk;
- initial and residual risk scores;
- details of the actions required to manage the risk;
- individual responsible for overall management of the risk;
- details of any resources required to manage the risk;
- timescales for risk review.

Risk assessors should include the following information asset threats in their review:

- Physical damage
- Natural events
- Loss of essential services
- Compromise of information
- Technical failures
- Unauthorised actions

- Compromised functions.

Approval of Risk Assessments

All completed risk assessments and action plans should be sent to the Managing Director for review.

Assurance and Incident Management

All information security incidents should be reported by following Telecom Advisor Ltd's Incident Reporting Procedure and should be logged.

Further information about incident reporting can be found in the Incident Reporting Policy and Procedure.

Information security incidents are reviewed by Telecom Advisor Ltd's Managing Director.

Secure Logon Procedures

All computer systems should have a logon authentication procedure that includes a unique user ID and password.

The following logon features should be considered:

- System/application identifiers should not be displayed until the logon procedure has been successfully completed.
- A 'pop up' window to prime screen use warning that the workstation should only be accessed by authorised users.
- No indication of which part of the logon information is incorrect.
- A limit of three unsuccessful attempts before locking users out.
- A limit for the maximum time allowed for logon.
- The system should record the date and time of successful logons linked to workstation identity.
- The password being entered is not displayed in clear text.
- Passwords should not be transmitted in clear text over the network.
- Systems should enforce password changes over a period of time.

Identifying and Authenticating Users

In order to facilitate and operate effective access control and audit functions it should be possible to:

- Uniquely identify all users of an information asset
- Group Identities/Generic Log Ons should only be approved if absolutely necessary and if approved by the Information Asset Owner in writing
- Where group identities are used a record of those users with access to the group should be held.

Password Policy

A Password Policy is used to establish rules concerning the use of passwords in the system.

The following criteria should be considered:

- Is it necessary to use group passwords on the system? Any group password usage will require approval by the Managing Director.
- Do users have to change their initial password (issued by the system administrator)? Users should be encouraged to set their own password, as it will usually be based on something they can remember.
- Are web browsers configured to prevent the recording of website passwords when logging in to web based applications? Recording of website passwords renders the password ineffective as a security measure. Passwords are therefore best if manually entered by the user at each login to be effective.
- Does the system log user passwords and prevent re-use? Repetitive re-use of passwords weakens the effectiveness of the password and should be avoided.
- Can users change their own passwords when they wish? This function increases security as users can change their password if they feel their current one has been compromised.
- Are complex passwords required? Simple passwords (less than 6 characters, number or letter only, repeated use) pose a threat to the system. Alphanumeric passwords of 6 characters or more should be considered for any system.
- Are periodic password changes enforced? A maximum period of three months between enforced changes is the norm for most systems.
- Are passwords displayed on the screen when being entered? Displayed password can obviously be seen by others and pose a security threat. Most systems now display only asterisks when characters are entered and some systems do not display anything. One of these latter rules should be implemented.
- Are passwords stored or transmitted in encrypted or hashed form? All passwords should be stored or transmitted using encryption or hashed.

Use of System Utilities

Some systems may include higher level accounts/security access groups that can override normal controls. The Information Asset Owner (or the delegated system owner or individual with equivalent responsibilities) will ensure that all system accounts are identified, disabled where necessary, and access using the system strictly controlled.

Information Access Restrictions

The integrity and availability of information is obviously important and should be considered by the Information Asset Owner (or delegated to the Information Asset Administrator). The ‘need to know’ principle of access should be supplemented with additional controls for altering or deleting information. File storage systems should be constructed with these criteria in mind, as in many cases, access to a folder allows the user to view, alter, copy and delete files in the folder (and Sub folders) unless they are protected.

Sensitive System Isolation

Systems holding data that is considered sensitive should be physically and logically protected from unauthorised access.

User Access Management

Telecom Advisor Ltd uses a wide range of locally based information systems. Some systems may allow all members of staff access whilst others restrict access to particular personnel.

It is essential that effective access management systems are in place for all systems, in order to prevent unauthorised access, loss or corruption of data, the introduction of malicious or unauthorised codes, and the abuse of access rights.

This standard applies equally to locally managed systems which process personnel data and to those that do not.

User Registration

The Information Asset Owner responsible for a system should be identified in the system level security policy. The policy should also identify the need for a formal registration/deregistration procedure, with restricted access for registering /deregistering users.

The registration process should ensure that the system can reliably identify the user. User authentication can vary in complexity depending on the sensitivity of the data to which the user may have access or depending upon the criticality of the system to Trust business

Computer system users should have a unique log on identity (ID), with a system and /or application log that shows logon/off times and activity.

Users' rights should reflect the business needs of the user. For example, some users may only need to view data, but not need to change or add to it. The system administrator should establish user profiles and manage user rights based on the 'need to know' criteria.

Users should acknowledge (digitally or in writing) 'acceptable terms of use' documentation or similar as part of the registration process. This should explain user rights in unambiguous terms and users should sign to acknowledge they have read, understood and agree to these terms.

User training documentation, guidance and the provision of user training sessions should be an integral part of the user registration process.

The Information Asset Owner should ensure that effective procedures are in place for deregistering users who no longer need access to the system. This includes people who no longer work for the organisation or have changed jobs.

A procedure should be available for temporarily suspending user accounts. This procedure may apply to those that have lost their log-on credentials, are suspected of misusing the system or are on long term sick leave/ leave of absence.

User Password Management

Use identification is the common means by which a user is identified to the system and therefore associated password creation, distribution and use should be strictly controlled.

If a password is being distributed electronically then it may be encrypted (this allows either an existing secure interface or an additional exchange process to allow the password to be decrypted by the intended users).

Systems should be configured to ensure that initial passwords issued to users have to be changed during the system's first access and regularly thereafter.

User passwords should be robust. As a minimum, passwords should:

- be no fewer than 6 characters
- be alphanumeric (mixture of letters, numbers and special characters (e.g. 5a!!AcY)
- be non-consecutive, (e.g. Pa55wOrD1 followed by Pa55OrD2 would not be allowed)
- have minimum enforced change periods established.

Systems users should be issued with written guidance on password confidentiality, construction, changing, storage and what to do if they forget a password. The guidance should also include instructions for reporting suspected password/identity misuse or the theft or the loss of log-on devices.

Review of User Access Rights

The Information Asset Owner should ensure that a written procedure is developed to regularly review all system user access rights. The review should be used to ensure users remain active and their access rights are allocated correctly. Six months is the recommended maximum period between such reviews although access reviews are best undertaken on a frequent basis and may be aligned with staff recruitment or movement cycles.

Social Networking and Blogging

There may be a requirement that some staff need to access social networking type services at Telecoms Advisor Ltd premises. Where such services are locally required, care must be taken to ensure that the information risks and management implications are appropriately considered. Telecom Advisor Ltd position is to restrict access unless a request for access is verified.

Unattended user Equipment and Data

A 'clear desk and screen' standard should be adopted for all systems to ensure that data is protected from unauthorised access. The Information Asset should ensure that this standard is written into security policy/procedures and training modules.

Users should lock access to their workstations when they are not using them at periods during the day, through the use of a password screensaver.

Paper and other media should also be locked away when not in use. This is especially important for media that contains personal details or other sensitive information.

Photocopiers and other multi-function office systems should be secured so that only authorised personnel may use them, for example password access systems. Digital copiers containing hard drives should be controlled in the same manner as required for other digital media, e.g. secure disposal.

Business Continuity Management

Business continuity is a core component of corporate risk management and emergency planning. Its purpose is to counteract or minimise interruptions to an organisation's business

activities from the effects of major failures or disruption to its Information Assets (e.g. data, data processing, facilities and communications).

Business Continuity Management (BCM) describes the company's attempt to predict, assess and counteract threats and risks that may cause or lead to significant disruption of all or part of the organisation's business functions. BCM examines the likelihood and impact of such disruptive events occurring, determines what the organisation can to do prevent or minimise the level of disruption and develop plans to affect systematic and timely recovery.

Telecom Advisor Ltd's Business Continuity Policy specifies the standards for business continuity management across Telecom Advisor Ltd.

The Information Asset Owner must ensure that they analyse the effect that particular disruptions might have on their information asset and link these into their risk assessment.

The Managing Director will liaise will the IAO/business continuity lead to ensure that information security elements are considered and reviewed.

Testing and Review

Business Continuity Plans should include information about how the plan will be tested. BCPs should be regularly tested and the outcomes documented through simulation exercises with plans refined or updated where necessary.

A review process should be established to review, coordinate and test the BCP. A regular review and testing schedule will be established, with both being conducted on an annual basis (minimum). Intermediate reviews should also be carried out following significant system changes, significant incidents, relocation of facilities and staff reorganisation.

Service Specific (Information Asset) Operation Measures

In addition to the Business Continuity Management overall programme the IAO (or equivalent) should identify measures to avoid or limit service-specific disruption of their business process. These measures should include:

1. Integrity and Availability of Data
2. Information Backup
3. Input Data – Validation
4. Control of Internal Processing.

Integrity and availability of data

The IAO must ensure that business data and software applications of their information assets are regularly backed up and tested using the system supplier's recommended technology and configuration.

The IAO must develop a risk-based back-up strategy that documents the procedures to be followed for each relevant information asset.

When the services of third party suppliers are used for data backup the IAO should ensure that arrangements conform to Telecom Advisor Ltd's information security and risk standards and the system supplier's recommended practices.

Information Backup

Business data is that data entered into one of Telecom Advisor Ltd's information assets, such as personal data or other files created and saved by users. Networked data is that stored on servers and should normally be backed up on a daily basis as a minimum by the system administrator or through automatic process.

Backup media for the previous week (or as locally agreed) should be compiled and stored securely, at a suitably controlled remote location to the server from which it was created. Consideration should be given to storing media in a different building or site to ensure it is protected if the location where the server is located is damaged thereby causing disruption or unavailability.

The back-up requirements may vary for different systems, therefore, it is a local decision for the IAO. However, Telecom Advisor Ltd recommends that a month's worth of data should be compiled and stored securely at a different location from the server.

The weekly and monthly storage media should be stored to protect them from unauthorised access and environmental threats such as heat, cold, magnetic fields and liquids. All media should be clearly marked to show the date the information was captured, the origin of the data and that it has been tested as reusable.

Instructions for backup should be made available in writing and more than one person should know how to carry out the backup and restore. A log should be kept of all start and finish times of backups, failed attempts and remedial actions, who carried out the backup and who has access to the media.

Media should only be used for the period recommended by the system supplier. It should be regularly tested to ensure that the data can be successfully recovered within the systems operational configuration. Redundant media should be securely destroyed using industrial strength tools.

Information that is not accessible from a network should be backed up on a daily basis and the media clearly labelled with the name of the responsible owner and stored securely. It is particularly important that individuals with data stored on individual work stations are aware of this and ensure that data is saved. Where possible data should be saved on networked servers and **no critical/sensitive data should be stored on stand-alone equipment.**

Local workstations should be configured so that a network drive is set as the default for the storage of data, rather than a local folder on the computer itself, such a 'My Documents' in Microsoft windows environments.

Input Data – Validation

Authentic data input is the responsibility of the person inputting the data supported by their line manager. All systems will include validation processes at data input to check in full or in part the acceptability of the data.

Systems owners should report all data errors together with a helpful reason for the error or rejection to facilitate its correction. Error correction should be done at the source of input as soon as it is detected.

Any loss or corruption of data should be reported immediately to the IAO who should report the incident in accordance with Telecom Advisor Ltd Incident Reporting Procedure.

Control of Internal Processing

.

All new systems must include controls that check for data corruption which has resulted from processing errors or other possibly deliberate acts. These controls should include:

- functions that are used to implement changes to existing information
- procedures to prevent programs running in the wrong order or running after the failure of a prior process
- programs to recover from failures
- protection against attacks that use buffer overruns/overflows
- error logging and reporting
- Protection from misuse of ‘on-line’ registration functionality.

The responsibilities of the system users with respect to checking data validity at input and output should be considered and defined. All user training should emphasise the importance of inputting accurate data.

Staff Awareness

Relevant information should be communicated to all staff to ensure that they are fully aware of business continuity plans and service specific procedures which affect them and their specific role in the recovery process. Testing and training needs to be conducted to ensure that staff know what to do if business continuity plans are activated.

Preventing Disruptions to Information Processing

Protection of equipment (including that used off site) is necessary to reduce the risk of unauthorised access to data and to protect against loss, damage, theft or compromise of Information Assets that would disrupt the company’s activities. Consideration should also be given to equipment siting. Special controls may be required to protect against physical threats, and to safeguard facilities, such as electrical supply and cabling infrastructure.

Power failures, water and fire damage, theft, electromagnetic radiation, explosions, vandalism and simple human error, such as unplugging a file server, are all causes of data processing/service disruptions.

The Information Asset Owner should ensure they risk assess these threats to their information asset and:

- establish suitable countermeasures
- document the countermeasures on the risk assessment form.

The individual responsible for the protection of the information asset should ensure that threats to services provided by third parties, or outsourced services, are taken into account within contracts and suitable controls and reporting procedures are put into place.

Disaster Recovery Planning

In the case of severe disasters (fire, flood, explosion etc) it may not be possible to operate systems from their normal locations. Therefore, it is essential that data processing continuity plans consider alternative accommodation to continue operations. Temporary accommodations on another site, facilities provided by a third party, or mobile processing facilities are all alternatives that should be considered.

The Information Asset should ensure that plans are in place to deal with such disaster scenarios.

Prevention and Detection of Malicious and Unauthorised Mobile Code

Software and computerised information processing facilities are vulnerable to the introduction and spread of malicious code, such as computerised viruses, network worms, Trojan horses, logic bombs and spyware. Users must be made aware of the dangers of unauthorised or malicious code.

The Information Asset should ensure appropriate controls exist to detect or prevent its introduction or spread. In particular, it is essential that effective precautions be taken to prevent, detect and remove malicious code and control mobile code.

Functionality

Systems under control of Telecom Advisor Ltd should be assessed to ensure that there is sufficient protection against the following:

- Malicious code
- Mobile code.

Safeguards

Anti-virus software is the first defence against malicious or mobile code but is only as good as the last update. New viruses are being produced daily so anti-virus software updates should be made frequently.

Security of Communication Networks

The secure operation of our networks, which span Telecom Advisor Ltd’s boundaries and beyond, requires that careful consideration be given to the management, data flows, legal implications, monitoring and protection. Additional controls are also required to protect sensitive information passing over public networks.

Security of Network Services

Network services should be subject to service level agreements or contracts, and the security features for the service identified, with the responsibility for maintenance, monitoring and reviewing of security features agreed by the IAO. Telecom Advisor Ltd should ensure that it includes the right to audit the services provided as part of the agreement.

Security features should be identified through risk assessment processes and subject to regular review and where necessary refinement. Typical security features to be considered include:

- Authentication, encryption and network controls
- Technical parameters required for secure network connections
- Access approval, restriction and revocation procedures.
- Anti-virus/malicious code detection, removal and prevention procedures
- Environmental controls to protect network equipment, i.e. from fire, flood.

Security of Remote Working and Mobile Computing

Standards for the use of portable devices and mobile computing equipment are available in the Portable Devices Policy.

Responsibilities

This section sets out the roles and responsibilities of individuals in ensuring compliance and monitoring of this policy.

Managing Director

The Managing Director of Telecom Advisor Ltd has overall accountability and responsibility for Information Governance. He is required to provide assurance, that all risks to Telecom Advisor Ltd, including those relating to information, are effectively managed and mitigated.

Information Asset Owner (IAO)

For information risk, the Information Asset Owner (IAO) is directly accountable to the Managing Director and will provide assurance that information risk is being managed effectively.

The Information Asset Owner should be aware of what information is held and the nature of and justification for information flows to and from assets for which they are responsible.

The IAO should also understand the scope and boundaries of the information asset(s), their approved purposes, who the users of the assets are and what their requirements for guidance and training may be, the criticality of the assets to Telecom Advisor Ltd, their dependency on other assets, and which other assets are dependent on them.

All Staff

All staff who create, receive and use information have responsibilities for the information security and quality of that information.

Compliance and Monitoring

Telecom Advisor Ltd’s Managing Director will be responsible for managing these monitoring arrangements.