# INFORMATION MANAGEMENT & SECURITY POLICY

**Introduction**

LITC is responsible for the security and integrity of all data it holds. LITC must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to LITC's assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security:

- A computer security incident is an event affecting the processing of computer usage adversely. This includes:
    - loss of confidentiality of information
    - compromise of integrity of information
    - denial of service
    - unauthorized access to systems
    - misuse of systems or information
    - theft and damage to systems
    - virus attacks
    - intrusion by humans
- Other incidents include:
    - Loss of ID badge/s
    - Missing correspondence
    - Exposure of Uncollected print-outs
    - Misplaced or missing media
    - Inadvertently relaying passwords

Ensuring efficient reporting and management of security incidents will help reduce and in many cases, prevent incidents occurring. More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

**Purpose**

Management of security incidents described in this policy requires LITC to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.
The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide Guidance on acceptable use of information, spaces, and technology

**Scope**

This policy applies to:

- LITC employees, partner agencies, contractors and vendors
- All LITC departments, personnel and systems (including software) dealing with the storing, retrieval and accessing of data
- All LITC students, service users and volunteers

**Policy Statement**

LITC has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing LITC employees, partner agencies, contractors and vendors of the importance of the identification, reporting and action required to address incidents, LITC can continue to be pro-active in addressing these incidents as and when they occur.

All LITC employees, partner agencies, contractors and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible via LITC's Incident Reporting procedures. The types of Incidents which this policy addresses include but is not limited to:

Computers left unlocked when unattended

Users of LITC computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All LITC employees, partner agencies, contractors and vendors need to ensure they lock their computers appropriately - this must be done despite the fact that LITC computers are configured to automatically lock after 5 minutes of idle time. Discovery of an unlocked computer which is unattended must be reported via LITC's Incident Reporting procedures.

Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, the Transformation Service must be notified through LITC's Incident Reporting procedures. For more information, LITC Password policy is available on the intranet or via the shared Server drive. Under no circumstances should an employee allow another employee to use their user account details after they have logged onto a system – even under supervision.

Virus warnings/alerts

All Desktop, laptop and tablet computers in use across LITC have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to LITC's data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to the IT Service Desk as soon as possible.

Media loss

Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device who has misplaced or suspects damage, theft whether intentional or accidental of any portable media must report it immediately through LITC's Incident Reporting procedures.

Data loss/disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised -recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on LITC's website and identified as inaccurate or inappropriate (which must be reported)
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill-advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function Devices
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All LITC employees, partner agencies, contractors and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of LITC'S data at all times.
Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using LITC's Incident Reporting procedures

**Personal information abuse**

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc… must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.
Any abuse/misuse of such person identifiable information must be reported through LITC's Incident Reporting procedures.

**Physical Security**

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower floor/level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the IT Service via LITC's Incident Reporting procedures.
Continuing emphasis and re-enforcement of LITC's Secure Desk policy will further help to reduce the number of security incidents.

**Logical Security / Access Controls**

Controlling, managing and restricting access to LITC's Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorized employees can gain access to information which is processed and maintained electronically.

**Missing correspondence**

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc… must be reported through LITC's Incident Reporting procedures.

**Found correspondence/media**

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through LITC's Incident Reporting procedures.

**Loss or theft of IT/information**

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc… or which is known/or suspected to have been stolen needs to be reported immediately through LITC's Incident Reporting procedures

**Responsibilities**

It is the responsibility for all LITC employees, partner agencies, contractors and vendors who undertake work for the LITC, on or off the premises to be proactive in the reporting of security incidents. LITC's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of LITC'S data and information.
It is also a responsibility of all individuals and handlers of LITC'S data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

Compliance with legal and contractual obligations.

- The Data Protection Act (1998) requires that personal data be kept secure against unauthorised access or disclosure.
- The Computer Misuse Act (1990) covers unauthorised access to computer systems.

**Breaches of Policy**

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to LITC's assets, including IT equipment and information, or conduct which is in breach of LITC's security procedures and policies.
All LITC employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through LITC's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of LITC.
In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of LITC's IT systems or network results from the non-compliance, LITC will consider legal action against the third party. LITC will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under LITC's disciplinary process or the relevant standards agencies in the case of elected members.
This Policy is referenced by other LITC policies and guidelines. Copies of these policy statements are obtainable via the LITC's Intranet or through the shared Server.

**Service Users and Students**

**Acceptable Use**
LITC devices must be used in accordance with their specific purpose and in line with the guidelines provided specifically by LITC staff and tutors.

**Safe Use of IT**

All devices available within LITC premises and/or made available to service users and students to carry out work related to LITC programmes must be used in line with our safeguarding policy with specific reference to the content relating to internet and media content.

No site or platform is restricted on any of our devices to allow full freedom in line with our mission, but browsing history and activity is monitored regularly and all members of staff and service users are required to report any concern to the lead safeguarding officer.

**Computer Based Assessments**

Students sitting for CBA sessions will receive detailed guidelines on what devices are allowed in the venue and if they are allowed to make use of personal devices during the assessment.

LITC devices used during assessments must be used in accordance with guidelines provided at the beginning of each session.

**REVIEW**

This policy and arrangements will be reviewed annually by the Quality Assurance Manager.

Reviewed By: Kum Chi On: 17/01/2023