School of Computing

# Security Policy and Incident Management

# Assignment 1

November 28, 2019

# Contents

# List of Figures

# List of Tables

# 1 Introduction

## 1.1 Overview

This information security policy document consists of various policies, aiming to safeguard Leading Edge Technologies' (LET) ability to achieve its business goals by minimising risks that threaten the confidentiality, integrity and availability of LET's information security. These policies implement both physical and logical measures, standards, rules and guidelines across LET premises, networks, IT systems and services in order to provide authorised, granular, auditable and appropriate user access.

## 1.2 Purpose

The policy statements within this information security policy are in place to protect the interests of LET and all its authorised users as well as to mitigate LET workstation-related risks such as — physical theft or damage to LET workstations or information assets, infection by viruses or other malware, unauthorized access, use and theft of confidential information. This is achieved by creating a safe, secure and accessible environment to work in.

## 1.3 Background

LET is a research facility which is an effort allowing various industries to tap on the talents and resources of Tsalach University (TU).

### 1.3.1 Business Goals of LET

LET aims to boost collaboration with industries to develop innovative solutions for various projects.

### 1.3.2 Assets of LET

**Physical Assets**

- 8 Desktop Workstations
- 3 Server Workstations
- 1 Colour Laser Printer
- 1 3D Printer
- Other Project Related Peripherals
- Off-site Backup Office

### Digital Assets

- Project-related information — including but not limited to proprietary designs, source code and project specifications.
- Personal particulars of LET staff
- Information on LET clients
- Other company related information

### 1.3.3 Network Architecture of LET

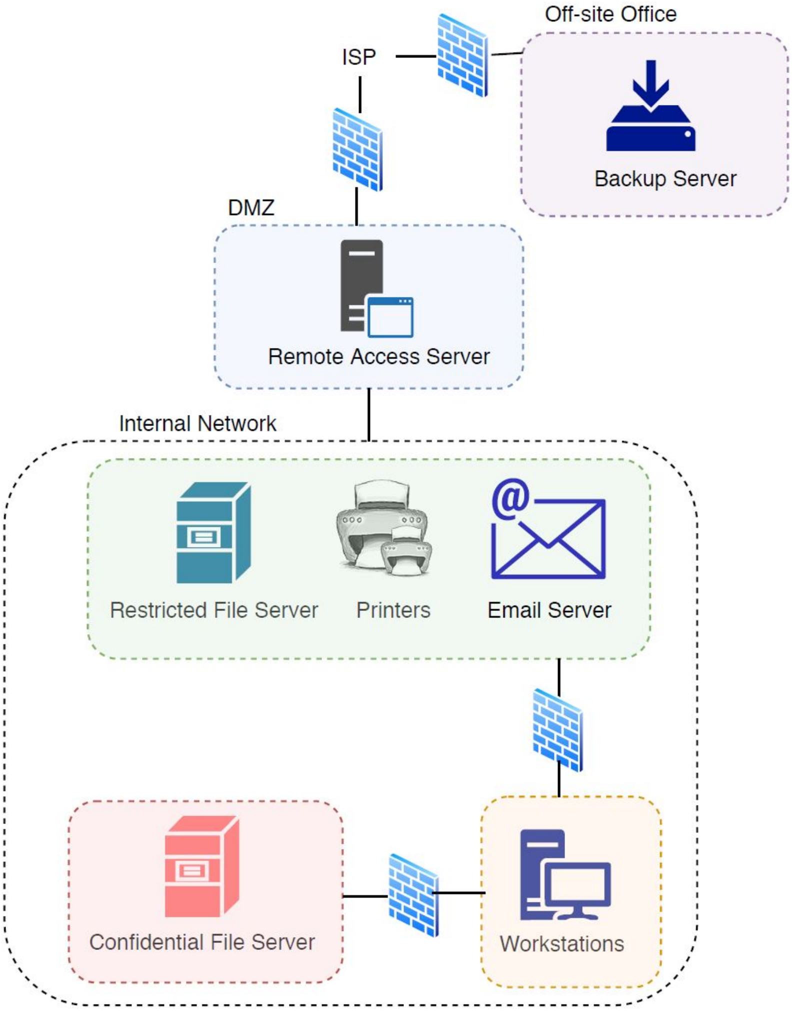

Figure 1: Network Infrastructure of LET

### 1.3.4 Company Hierarchy

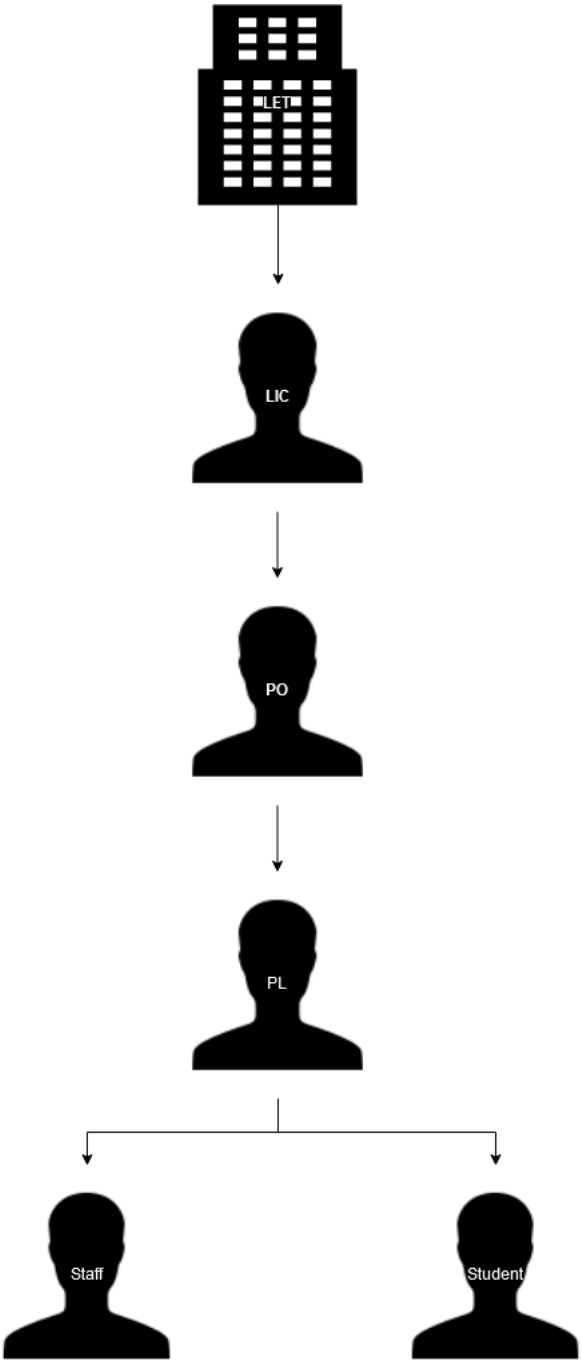

Figure 2: LET Hierarchy

## 1.4 Scope

This policy document applies to all users in LET. This includes the staff and students of Tsalach University (TU) whom are users of LET as well as visitors that have temporary access. This policy document also covers all desktop workstations, network servers, and other computing equipment within LET.

## 1.5 General Definitions and Terms

For the purpose of the document, the following definitions apply to all information security policies.

| **Term** | **Definition** |
|---|---|
| LIC | Lecturer-in-Charge |
| PL | Project Leader |
| PO | Project Officer |
| Students | TU students who are part of the projects in LET. |
| Users | "Users" refers to the PO, the LIC, PL's, LET staff and Students. |
| Computer Equipment | All network and workstation related hardware and peripherals owned or leased by LET and its subsidiaries. |

Table 1: General Definitions and Terms

## 1.6 Disclaimer

This information security policies in this document are based on assumed information about LET documented above.

# 2 Revision History

| Version No. | Date Of Change | Responsible | Description |
|---|---|---|---|
| 1.0 | 13/11/2019 | Ahuv Consulting Pte Ltd Policy Team | Initial Version |

Table 2: Revision History

# 3 Policy Statements

## 3.1 Data Security Policy

### 3.1.1 Overview

Information accessed, stored or created by LET is a valuable asset to the LET and also Tsalach University along with its industry partners. Unauthorised use could pose adverse consequences for individuals and subject the LET and TU to legal action and government or federal sanctions.

### 3.1.2 Purpose

The policy intends to outline the data classification of proprietary information, its respective protection measures and also data retention procedure for each data category. The rules intend to protect the intellectual property of LET. Improper handling of the data thus exposes the LET to data theft or alteration which would impede and hinder the business goals of LET.

### 3.1.3 Scope

This policy applies to everyone creating, accessing, modifying and storing information belonging to LET (including but not limited to all Users, visitors, contractors, consultants, temporary staff and affiliates of the LET.).

This policy also applies to all storage media, storage servers or the like, containing proprietary information belonging to LET, owned or leased by LET or is registered under a LET owned internal domain network.

### 3.1.4 Policy

1. **Data Classification**

   LIC and PO are responsible for segregating and classifying the data and information assets according to the classification system presented as follows.

   Where practical, information classes are to be embedded in the information itself (watermarking).

   (a) **Data Importance**

   All proprietary information may be grouped into the the following three levels of importance:

   i. **Low**

      Information is of low importance to the ability of LET in conducting its business goals. Loss of availability due to system downtime is acceptable. Integrity of the information is important but not vital.

   ii. **Medium**

      Unauthorised access to the information could influence LET's operational effectiveness, cause important financial losses, provide significant gains and advantage to competitors or cause a major drop in customer confidence. Information integrity is vital.

   iii. **High**

      Information in this category is of the highest importance and directly influences LET's ability to conduct its business. Highest levels of integrity, confidentiality and restricted availability is crucial to ensure LET is able to meet its business goals.

(b) **Data Classes**
Based on their importance, LET information will fall into one of the three following categories:

   i. **Unclassified Public**

      A. Information determined to be of low importance will fall in this class.

      B. Unclassified public information may be accessed, used, shared or modified by anyone within or outside of the LET. The LET must be credited for any use of information that it has created.

      C. Examples of Unclassified Public Information include but are not limited to widely distributed product brochures, information available in the public domain, sample downloads of company software that is being distributed, financial reports required by regulatory authorities and newsletters for external transmission.

   ii. **Restricted**

      A. Restricted information constitutes information of medium importance.

      B. Information in this class can only be accessed by authorised users in the LET.

      C. Sharing of restricted information is only allowed between LET staff and only if necessary for the recipient in the course of his work.

D. Authorisation is granted to users by the LIC and PO.

E. Information in this class can be accessed through the workstations in the LET facility or remotely. Remote access requirements are detailed in the *Remote Access Policy* .

F. Examples of Restricted Information include but are not limited to project specifications and briefs, company emails sent using the LET email server and standard operating procedures used in all parts of the LET.

iii. **Confidential**

A. Confidential information contains information of the highest importance.

B. Information can only be accessed by authorised users of the LET.

C. Authorisation is granted to users by the LIC and PO.

D. Original copies of the information cannot be modified or changed without permission from the PO or LIC (or the client if dealing with client confidential data).

E. Confidential information can only be accessed from within the LET network. Sharing of information is strictly prohibited.

F. Examples include but are not limited to client media, electronic transmission and communications with clients, salaries and personnel data, designs and solutions created by the LET and project-related files.

Acceptable use of any and all data is detailed in the *Acceptable Use Policy.*

2. **Data Retention**

(a) **Data Storage**

i. **Unclassified Public**

Storage of unclassified public data is unrestricted and is left to the discretion of the LET users so long as it complies with the *Acceptable Use Policy*, *Physical Security Policy* or other policies that may be involved.

ii. **Restricted**

A. Storage of Restricted data is limited to the restricted data servers and the email server.

B. Restricted data may only be communicated in person or via the company email.

C. Restricted data must not be circulated outside of the LET.

iii. **Confidential**

A. Storage of confidential data is restricted to the confidential file server.

B. Confidential data must only be communicated in person.

C. Permission of the LIC and/or PO must be sought in order to make copies of the confidential document be it physical or digital.

D. All physical copies of confidential documents must be destroyed after use.

E. All digital copies of confidential documents must be deleted using secure deletion methods.

iv. **Data Encryption**

A. **Restricted**

All restricted information must be encrypted using encryption standards approved by the LIC and PO while in motion.

B. **Confidential**

All restricted information must be encrypted using encryption standards approved by the LIC and PO while in motion and at rest.[5][6]

## 3.2 Acceptable Use Policy

### 3.2.1 Overview

The intention of the LET Acceptable Use Policy is to protect TU staff and students using the LET facility, industry project partners, LET and Tsalach University from damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to Computer Equipment, WWW browsing, and FTP, are the property of LET. These systems are to be used for developmental purposes in serving the interests of LET and its partners in the course of normal operations.

Effective security is a team effort involving the participation and support of every user and affiliate of the facility who deals with information and/or information systems. It is the responsibility of all users to know these guidelines, and to conduct activities within the LET accordingly.

### 3.2.2 Purpose

The purpose of this policy is to outline the acceptable use of information and Computer Equipment of LET. These rules are in place to protect the LET facility users, LET and TU. Inappropriate use will thus expose LET and TU to risks including virus attacks, compromise of network systems and services and legal issues.

### 3.2.3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources for normal LET operations or to interact with internal networks and systems owned or leased by LET, the users, or a third party. All users of LET are responsible for exercising good judgment regarding appropriate use of information, electronic devices and network resources in accordance with LET policies and standards and local laws and regulation.

This policy applies to all Users, contractors, consultants, temporaries, and other workers at LET, including all personnel affiliated with third parties. This policy applies to all equipment owned or leased by the LET.

### 3.2.4 Definitions and Terms

| Term | Definition |
|---|---|
| Proprietary Information | Information that is unique to LET and its ability to compete. This includes but is not limited to project-related files regardless of its data class specified in the Data Security Policy, project designs and solutions |
| Blogging | Any post, entry or upload not limited to written or pictorial on any sort of social media or sharing platform on the internet. |
| Honeypots | Simulate one or more network services on a decoy machine or computer, luring attackers to attempt to attack this seemingly vulnerable machine. Upon entry into this dummy computer or server, the attackers movements may be logged and observed. |
| Honeynets | Similar to honeypots except that rather than simulating a single computer, it simulates an entire decoy network. A honeynet would house many honeypots. |
| Spam | Electronic junk mail or junk newsgroup postings. This includes but is not limited to unsolicited advertisements on any sort of electronic media. |

Table 3: Acceptable Use Policy Definitions and Terms

[14]

### 3.2.5 Policy

1. **General Use and Ownership**

   (a) LET proprietary information stored on electronic and computing devices whether owned or leased by LET, the employee or a third party, remains the sole property of LET. All proprietary information must be protected in accordance to the Personal Data Protection Act through legal or technical means.

   (b) Responsibility lies on the individual to promptly report the theft, loss or unauthorised disclosure of LET proprietary information.

   (c) Users, contractors, consultants, temporaries, and other workers at LET dealing with proprietary information will be required to to sign an NDA prior to job or task commencement.

   (d) Access and use of proprietary information is granted only to the extent it is authorised and necessary to fulfill assigned tasks and job duties.

   (e) Sharing of proprietary information is strictly prohibited as stated in the Data Security Policy unless an exception is made and approved by the LIC or PO.

(f) Failure to keep LET proprietary information confidential will result in breach of the NDA and legal action will be taken against the perpetrator.

(g) All employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their superior for clarification.

(h) For security and network maintenance purposes, authorised individuals within the LET may monitor equipment, systems and network traffic at any time, per the Audit Policy.

(i) LET reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. **Security and Proprietary Information**

(a) All LET Computer Equipment connected to the LET internal network must be used in compliance with the respective policies.

(b) All non-LET Computer Equipment, for example mobile and computing devices, are not allowed to connect to the LET internal network.

(c) System and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

(d) Postings by Users to newsgroups or any website should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the LET, unless posting is in the course of business duties.

3. **Email Use**

(a) Access of the LET email account must only be from within the internal network and any outgoing emails to non-LET domains must not contain and restricted information as defined in Data Security Policy.

(b) Emails should be made with the appropriate signatures and designation clearly displayed in the footer or any appropriate location within the email and must be encrypted with LIC and PO approved encryption standards.

(c) Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4. **Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of LET authorised to engage in any activity that is illegal under local, state, federal or international law while utilising LET-owned resources.

The lists below are by no means exhaustive, but attempt to provide a guideline for activities which fall into the category of unacceptable use.

(a) **System and Network Activities**

    The following activities are strictly prohibited. Under no circumstances will exceptions be granted.

    i. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by LET.

    ii. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which LET or the end user does not have an active license is strictly prohibited.

    iii. Accessing data, servers or accounts for purposes outside conducting LET business is prohibited even if authorisation is given.

    iv. Introduction of malicious programs (e.g., malware, logic-bombs, key loggers, etc) onto LET workstations, servers or network.

    v. Revealing LET account passwords to others or sharing of accounts is prohibited. This includes family members and other household members if work is remotely done from home. Please refer to the Remote Access Policy for remote access requirements.

    vi. Using LET assets to actively engage in procuring or transmission of contraband material that is in violation of sexual harassment or hostile workplace laws is prohibited.

    vii. Making statements about warranty, expressly, or implied, unless it is part of normal job duties.

viii. Attempt or effect security breaches or disruptions of network communications. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping flooding or sweeping, packet spoofing, denial of service, and forging or spoofing routing information for malicious purposes.

ix. Port scanning or security scanning prior to informing PO or LIC.

x. Network monitoring involving the intercepting of data not intended for the employee's host, unless part of employee's normal course of duty.

xi. Introducing honeypots, honeynets or other similar decoys onto the LET network.

xii. Interfering or denying service of LET servers or other Users' workstations

xiii. Using programs, scripts, commands or sending messages of any sort with the intent to interfere, disable, terminate or modify a User's terminal session locally, remotely or via any means.

xiv. Providing information about LET employees to parties outside LET.

(b) **Email and Communication Activities**

When using company resources to access and use the Internet, users must be aware that they represent LET. Whenever stating affiliation to LET, users must indicate that "the opinions expressed are my own and not necessarily those of the company".

i. Sending unsolicited emails, including "junk mail" or other advertising material to individuals without their request. (Spam)

ii. Any form of harassment via email, telephone, instant messaging or any other communication platforms, whether through language, frequency or message size.

iii. Unauthorised use, forging or spoofing of email header information.

iv. Solicitation of other email addresses with the intent to harass or gather responses.

v. Creating or forwarding "chain letters" or other "pyramid" schemes.

(c) **Blogging and Social Media Use**

i. Blogging by employees, be it using LET's property and systems or personal devices, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of LET's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate LET's policy, is not detrimental to LET's best interests, and does not interfere with an employee's regular work duties. Blogging from LET's systems is also subject to monitoring.

ii. LET's data security policy also applies to blogging. No confidential or restricted information covered by the Data Security Policy should be revealed in blogging.

iii. Any blogging that may harm or tarnish the reputation and/or goodwill of LET and/or any of its employees. Employees are also prohibited from making discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct that could constitute to discrimination, harassment or any prejudice behaviour.

iv. Employees assume any and all risk associated with blogging. Employees may not attribute any personal statements, opinions or beliefs to LET. When expressing personal beliefs and opinions, users are not to represent themselves as employees, representatives or affiliates of LET.

v. Apart from compliance to laws pertaining to the handling and disclosure of copyrighted materials, LET's trademarks, logos and any other intellectual property may also not be used in any blogging activity.[13]

## 3.3 Physical Security Policy

### 3.3.1 Overview

The LET Physical Security Policy is implemented in order to ensure the safety of the LET's computer and physical resources on the company's premises.

### 3.3.2 Purpose

This policy is intended to ensure that physical computer resources and information resources are properly protected physically from damages caused by human or the environment.

### 3.3.3 Scope

This policy applies to all physical assets owned, operated, maintained and controlled by LET.

### 3.3.4 Policy

1. **Environment**

   The temperature and humidity of the location are to be maintained at the operating levels of the equipment in the location to prevent equipment from malfunctioning.

2. **Access Control System**

   Access control systems are to be provisioned and deployed for any area requiring physical access into a facility, or within the facility. As a physical security protection measure, and to ensure that access to LET facilities are only given to authorised individuals with access rights. Additionally, all access must be logged either electronically or through log sheets. [12]

| **Personnel** | **Office** | **Restricted Server Room** | **Confidential Server Room** | **Offsite Office** |
|---|---|---|---|---|
| LIC | O | O | O | O |
| PO | O | O | O | O |
| PL | O | O | X | X |
| Staff | O | X | X | X |
| Student | X | X | X | X |
| Visitor | X | X | X | X |

Table 4: Access Rights

*Note: This access rights is only for the individual, meaning when they try to access the facility on their own.*

3. **Facility Access**

   Only authorised personnel with the valid access rights will be allowed access to the applicable facilities.

   Information, such as full name, contact information, company affiliation, along with date and time of entry and departure to and from the facility, and any other useful information must be logged either electronically or on log sheets. This allows anyone in the facility to helping in determining if access controls have been breached.

   Labelled key card with the corresponding access rights of the personnel will be issued and has to be clearly visible for identification of the type of personnel they are. [12]

   Depending on the personnel type there may be access restrictions that applies, refer to table 5.

| **Personnel** | **Personnel Type** | **Restrictions** |
|---|---|---|
| LIC | Authorized Staff | NIL |
| PO | Authorized Staff | NIL |
| PL | Authorized Staff | NIL |
| Staff | Authorized Staff | NIL |
| Student | Unauthorized Staff | Accompanied by an PO or LIC at all times. |
| Visitor | Visitor | Accompanied by a PL at all times. |

Table 5: Personnel Types

4. **Lock Down**

   Office premises must be secured in the absence of an authorised staff, with all physical locks on entryway doors engaged. [2]

5. **Surveillance**

   Cameras are to be strategically placed throughout the facility as deemed necessary to record all activity. Additionally, this requires the use of monitoring devices whereby authorized personnel can view footage in real-time. Archival measures are to be in place for retention of data caught on camera in accordance to *Disaster Recovery and Backup Policy.* [12]

6. **Server Room**

   Server equipment are to be placed in secured rooms where additional physical access controls are put in place to enforce stronger physical security, such as placing an physical key lock as an second lock in addition to an digital key card lock.

7. **Provisioning of Keys**

   Provisioning of keys, key cards or any other form of a key must be logged either electronically or through log sheets with the format as follows:

   - Description of key provided
   - Recipient of key
   - Provider of key
   - Date approved
   - Duration of provision

8. **Equipment**

   Removal or addition of any equipment belonging to LET in the facility must be logged and accounted for. [2]

9. **Equipment Checks**

   Any person entering or leaving the facility are to be checked for prohibited items in their possession. Bag checks, pat downs and any other checks deemed necessary are to be employed. [12]

10. **Prohibited Items**

    These types of devices are prohibited unless approved by PO or LIC. In the case of mobile phones the cameras has to be physically removed to be brought in.

    - Storage devices
    - Data Cables
    - Image Capturing Devices

## 3.4 Software Security Policy

### 3.4.1 Overview

Allowing Users to install software on company computing devices may result in unauthorised access and use of the organisation's confidential data. For example, conflicting file versions or DLLs which may prevent programs from running properly or entirely, the introduction of malware to LET's network from malicious installation software, and the discovery of unlicensed software during an audit.

### 3.4.2 Purpose

The purpose of this policy to outline the configurations requirements and standards around software on LET computing devices. The main focus is to elaborate on minimising the risk of loss of program functionality, the exposure of confidential contained within LET computing network and the risk of introducing malware to the company network.

### 3.4.3 Scope

This policy applies to all Users who have authorised access to a LET owned workstation. This policy covers all computers, servers and other computing devices operating within LET.

### 3.4.4 Definition and Terms

| Term | Definition |
|---|---|
| Software | Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.[14] |

Table 6: Software Security Policy Definitions and Terms

### 3.4.5 Policy

1. **Workstation Configuration**

   (a) Each domain workstation shall be configured to use Windows 10 as its operating system, and contain a standardised set of software applications as listed below:

   - Chrome
   - Firefox
   - Java SE 8 Update 65 or higher

- Open Office
- Adobe Acrobat Reader

(b) Each domain workstation must be configured to have an Administrator account, and only the LIC and PO will be given access to the Administrator account.

(c) Each domain workstation must be configured to only allow software installation or configuration modification to be performed by the Administration account.

(d) Computer Equipment must be set to automatically lock if unused within 10 minutes or less where possible.

(e) All software logs must be forwarded and stored in the confidential network server for auditing purposes stated in the *Security Audit Policy*.

(f) Each workstation must have antivirus installed and must be updated regularly.

2. **Software Requests**

(a) All software installation requests must be reviewed and approved by the PO first.

(b) All software from software requests must be selected from an approved software list, which shall be maintained by the PO, unless no selection on the list meets the requester's need.

(c) All software requests shall be logged and accounted for.

(d) All requests within a project should be collated by the respective PL before submitting a software request for review.

(e) The PO will obtain and track the licenses, test new software for conflict and compatibility, before performing the installation.

(f) All installed software must be updated to the latest secured version, unless if the update prevents the program to run properly or entirely.[19]

## 3.5 Server Security Policy

### 3.5.1 Overview

Proprietary LET information is stored in and transmitted through critical workstations that run server software. These servers, if vulnerable, can be a major entry point for malicious threat actors. Consistent server installation policies, ownership and configuration management are about nailing the basics.

### 3.5.2 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by LET. Effective implementation of this policy will minimise unauthorised access to LET proprietary information and technology.

### 3.5.3 Scope

All users of LET must adhere to this policy. This policy applies to server equipment, operated or leased by LET or registered under a LET-owned internal network domain, as well as any network equipment interacting with the server equipment.

### 3.5.4 Definitions and Terms

| **Term** | **Definition** |
|---|---|
| Server | A computer or computer program which manages access to a centralised resource or service on a network, as well as the hardware required for the server in question to function and the firewall that protects the server. |

Table 7: Server Security Policy Definitions and Terms

### 3.5.5 Policy

1. **General Server Requirements**

   (a) All internal servers deployed at LET must be owned by the PO who is responsible for system administration. Server configuration guides must be established and maintained by the PO. The PO should monitor configuration compliance and implement an exception policy tailored to the environment.

2. **Configuration Requirements**

   (a) Services and applications that will not be used must be disabled where practical.

(b) Access to services should be logged and/or protected through access-control methods in-line with the guidelines as follows:

   i. Remote Access to servers is strictly prohibited

   ii. Access to servers must utilise two-factor authentication methods

   iii. Passwords to accounts used to access workstations running server software must adhere to the standards set in the *Password Protection Policy*

(c) The most recent security patches must be installed on servers as soon as practical, the only exception being when immediate application would interfere with business requirements.

(d) Information must be securely stored and transmitted through the encryption standards defined in the Data Security Policy.

(e) Always use standard security principles of least required access to perform a function. Do not use a root account when a non-privileged account will do.

(f) Preventive measures against disruptions to the availability of servers must be taken:

   - Servers should be physically located in an access-controlled environment, with preventive measures against environmental harm as defined in the *Physical Security Policy*
   - Servers must run in high-availability clusters.
   - Uninterrupted power supplies must be provided in the event of a power outage.

(g) Functions meant to scrutinise incoming and outgoing traffic for data leakage (eg. Data Loss Prevention (DLP) features on firewalls) must be enabled where available.

(h) Servers must be hardened according to a hardening guide, if available, subject to the approval of the PO and LIC.

3. **Monitoring**

(a) All security-related events on Server with must be logged and audit trails saved to the centralised Confidential file server following the standards set by the *Data Recovery and Backup Policy* [18]

## 3.6 Password Protection Policy

### 3.6.1 Overview

Passwords are a critical aspect of computer security. A poorly chosen password may cause unauthorised access and/or compromise of the organisation's information assets. All authorised Users with access to LET systems are responsible for taking the appropriate steps, as outlined below, to select and secure LET accounts' passwords.

### 3.6.2 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords and the protection of those passwords.

### 3.6.3 Scope

The scope of this policy includes all Users who have or are responsible for an account (or any form of access that supports or requires a password) on any computer system that resides at any LET facility, has access to the LET network, or stores any non-public LET information.

### 3.6.4 Policy

1. **Password Creation**

   (a) All user-level and administrator-level passwords must be made up of a minimum of eight alphanumeric characters, containing at least one letter and one numeral.

   (b) All Users' passwords must not be the identical as the account ID or user ID.

   (c) All Users' passwords must not contain any information related to the company.

   (d) User accounts that have administrator-level privileges must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

   (e) Users must not use any work related passwords for any personal accounts

2. **Password Change**

   (a) All Users' passwords must be changed at least every ninety days.

   (b) All Users must not reuse at least three generations of password upon a password change request.

(c) New users are required to change password upon the first login, while adhering to the password creation guidelines above in the *Password Creation* section.

3. **Password Protection**

    (a) Passwords must not be displayed in clear. This means that passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as confidential LET information.

    (b) All Users shall be locked out from their account after three failed login attempts.

    (c) All Users suspecting that LET account's password might have been compromised must report the incident and change all passwords belonging to their LET account.[15]

## 3.7 Remote Access Policy

### 3.7.1 Overview

Remote access to LET internal network allows Users to read or write restricted information like LET internal emails, project specifications and personal particulars as defined in *Data Security Policy*, from various locations. Benefits of remote access, namely better convenience, higher productivity, more agile business process and lower travel cost, are paramount in boosting LET's efficiency.

However, the security posture of the remote networks and computers which remote access originates from is often beyond the control of LET which will pose significant risks on the information security of LET.

### 3.7.2 Purpose

The purpose of this policy is to set the standards that Remote Access must adhere to at any time. The standards are devised to minimize the risks posed by Remote Access including but not limited to loss or illegal alteration or leakage of Restricted Data, damage to internal servers and financial liabilities incurred as a result of these.

### 3.7.3 Scope

The policy applies to all Users who are authorised to Remotely Access any Computer Equipment in LET's internal network (hereafter referred to as "Authorised Users"). The policy defines the rules of Remote Access which Users should follow and their responsibilities. Furthermore, the policy specifies any and all technical requirements of LET's Remote Access implementation.

### 3.7.4 Definitions and Terms

| **Term** | **Definition** |
|---|---|
| Remote Access | The access to LET's private LAN using external computers from any locations outside LET's firewall via the Internet. |

Table 8: Remote Access Policy Definitions and Terms

### 3.7.5 Policy

1. **User Responsibilities** [1][16]

   (a) Authorised Users must never share their login credentials with anyone, including family members.

(b) Authorised Users must verify that they are using the Remote Access technology as specified by LET and its software is the latest secured version.

(c) Authorised Users must take necessary steps in ensuring the computers they use for Remote Access are free from threats such as virus, malware and worms. These steps include but not limited to installation of the latest security patches for the operating system and make sure the antivirus software running has the latest virus definitions.

(d) Authorised Users should must not be connected to any other network during Remote Access, unless they have complete control over the network like their private home network.

(e) Authorised Users must treat Remote Access connections with the same security consideration as their computer connection within LET's premises.

(f) Authorised Users must prevent any unauthorised user from accessing LET's internal network using their established Remote Access session.

(g) Authorised Users must not use Remote Access for any purpose that is outside LET's business interest and all usage should comply with *Acceptable Use Policy.* Authorised Users bear the full consequences should the Remote Access be misused.

2. **Technical Requirements of Remote Access** [1][16]

   (a) Confidential Data defined in *Data Security Policy* cannot be accessed via Remote Access.

   (b) Remote Access' implementation must use either Virtual Private Network (VPN) or Microsoft Remote Desktop Service (RDS) technology which should be the most-up-to-date secured version. [20][23].

   (c) Remote Access's connection via VPN or RDS must follow the encryption standards for Restricted Data specified in *Data Security Policy.*

   (d) Remove Access's implementation must be configured to follow the latest hardening guidelines of the technology chosen.

   (e) Two-factor authentication must be used for Remote Access. Two-factor authentication should use two out of the following three forms of authentication:

      - Something known to the Authorised User; e.g. a strong password that complies with Password Policy.

      - Something processed by the Authorised User; e.g. mobile phone or a token device.

- Something unique to the Authorised User; e.g. fingerprint.

## 3.8 Disaster Recovery and Backup Policy

### 3.8.1 Overview

Leading Edge Technologies (LET) business goals are reliant on steady and constantly available Information Technology (IT) systems. Effective recovery plans must be established such that IT services can be resumed to an acceptable level within a required time frame in the event of a system disruption or disaster.

### 3.8.2 Purpose

The objective of this policy is to define the requirements for IT continuity, backup and recovery, for the purpose of preventing or mitigating the risk of an IT system disruption or disaster, and allow for the recovery of IT services and data in an efficient and timely manner.

### 3.8.3 Scope

This policy applies to all IT systems or applications managed by LET that store, process or transmit information, including network and computer hardware, software and applications.

### 3.8.4 Definitions and Terms

| **Term** | **Definition** |
|---|---|
| Disaster Recovery Plan (DRP) | A documented plan that describes the strategy to restore minimum IT services, application and data to resume critical business operations within a pre-defined period of time, and to fully recover such operations after a disaster affecting normal IT services. |
| Minimum Business Continuity Objective (MBCO) | The minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption. |
| Recovery Point Objective (RPO) | The maximum targeted period in which data might be lost from an IT service during a disruption. |
| Recovery Time Objective (RTO) | The targeted duration of time within which a business process must be restored after a disruption in order to avoid unacceptable consequences associated with a break in business continuity. |

Table 9: Disaster Recovery and Backup Policy Definitions and Terms

### 3.8.5 Policy

IT Continuity, backup and recovery must be managed in accordance with the guidelines contained in this policy.

Procedures and technology must be in place to ensure:

1. Prevention against IT system disruption
2. Regular and comprehensive backup of critical systems, applications and data
3. Timely recovery of critical systems, in-line with an RTO & RPO of 24 hours after a significant disruption.

### 3.8.6 Disaster Recovery Guidelines

1. A Disaster Recovery Plan(DRP) must be formally documented and contain the following details:
    - Step-by-step procedures to recover critical IT systems and applications and restore data after a major disruption. These must be in-line with the MBCO.
    - Clear roles and responsibilities
    - List of critical systems and applications that are aligned with business goals
    - Detailed minimum requirements and specifications for critical IT system components, including mapping of critical applications and data hosted on servers
    - Salvage list of the most important items to be recovered in an emergency, including the location of the asset
    - Contact information of key resources, including phone numbers (daytime and non-working hours), email and physical address where possible for.
        - The IT emergency response team
        - Other IT contacts (IT Staff, third-party IT supplier, application vendors, etc).
        - Other business contacts (application and system owners and administrators, key suppliers, customers and stakeholders, communication team, etc)
2. The DRP plan must be reviewed and tested in accordance to the *Security Audit Policy.* Regular tests of the DRP may include following:
    - High-level plan walkthrough
    - Table top exercise

- Simulation test
- Test of the communication channels and call notification procedures
- Data backup restoration

3. A copy of the DRP plan must be available off-site(using a laptop for example) and on-site at each LET facility.

#### 3.8.7 Backup Guidelines

1. **Generic Backup Requirements**
   (a) Contingency IT equipment must be in place where appropriate
   (b) Backups of LET Facility equipment must cover:
   - System Configuration and Data files on critical systems (ie. Windows Domain Controller)
   - Confidential and Restricted Data files stored on running servers
   - Configuration files for essential network equipment (ie. Firewalls)

2. **Backup Routines**
   (a) The following approach, based on a Grandfather-Father-Son (GFS) schedule provides the minimum requirements for the backup of critical IT systems.
   i. Daily Backups. Differentials or incremental backups.
   ii. Weekly backups. Full backups.
   iii. Monthly backups. Full backups.

   (b) Daily backups are performed each day. The following backups are performed daily:
   i. File-level backups copied from disk to an off-site backup server.
   ii. Daily backups are swapped and retained via a First-In-First-Out (FIFO) System with a retention period of 7 days.

   (c) Weekly backups are performed each weekend, during non-working hours. The following is performed:
   i. File-level backups copied from disk to removable backup tape media.
   ii. Weekly backup media are stored off-site and retained for a minimum of 4 weeks.

   (d) Monthly backups are performed each month. The following is performed:

      i. File-level backups copied from disk to removable backup tape media.

      ii. Monthly backup media are stored off-site and retained for 3 months.

3. **Physical security of backup media and contingency IT equipment**

   (a) Fallback or contingency equipment and backup media must be stored off-site at a sufficient distance to escape any damage from a disaster at the main site.

   (b) Long-term storage or backup data must meet the same basic physical and environmental control requirements in place for the critical IT systems, as outlined in the *Physical Security Policy.*

   (c) Appropriate care of all backup media must be taken to preserve their integrity.

      - Tapes must be stored according to the vendor recommendations.
      - Tapes must not be exposed to sources of contamination, such as copiers and printers that emit toner and paper dust, or high voltage electrical equipment.

   (d) Backup media reaching the end of their retention period must be fully erased and recycled in the pool of available backup media.

   (e) Any damaged, corrupted or end of life tapes must be destroyed.

   (f) All backup media must be labelled and identified with a unique identifier.

   (g) A detailed inventory must be maintained at all time to track the position and status of all backup media. The use of an automated inventory system is acceptable but must be completed with the regular verification of the true position and status of backup media.

   (h) Every physical transfer of backup media off-site must be formally tracked with the following criteria:

      - Date and time of transfer
      - Origin and destination locations
      - Name of the person taking the responsibility of the transfer
      - Detailed inventory of the media being transferred

   (i) Backup media stored off-site must be encrypted with standards defined in the Data Security Policy.

   (j) Security controls must be implemented to prevent access to backup management systems, backup files and backup media as defined in the Physical Security Policy.

### 3.8.8 Recovery Guidelines

1. **Standard Restoration Process**

   - All restore requests must be formally requested to the PO, who will detail the following:

     (a) Specific file(s) and/or folder(s) that are required to be restored.

     (b) From which server

     (c) From which specific data

     (d) To what restore location

     (e) Whether the restored data should overwrite the current data in the original location or not

   - A detailed procedure for data restoration must be documented, including the restoration of data stored in both on-site and off-site backups.

2. **Emergency Restoration**

   - Emergency Restoration must be formally initiation by the LIC.

   - Due care must be followed to prevent any loss of data or damage to backup media in an emergency.

   - Details of the backup restoration must be formally documented by the PO after the emergency. [3]

## 3.9 Incident Response Policy

### 3.9.1 Overview

It is vital to LET that security incidents that threaten the security or privacy of Confidential information are properly identified, contained, investigated, and remedied.

### 3.9.2 Purpose

The purpose of this policy is to provide the basis of appropriate response to incidents that threaten the confidentiality, integrity and availability of LET assets.

This Incident Response Policy provides the formal guidelines to creating Incident Response Procedures.

### 3.9.3 Scope

This policy applies to all Users of LET, as well as any other contractors, consultations, temporary workers, visitors and affiliates that hold information on LET assets.

### 3.9.4 Definitions and Terms

| Term | Definition |
|---|---|
| Incident Response Procedure (IRP) | A systematic and documented method of approaching and managing situations resulting from IT security incidents or breaches. |

Table 10: Incident Response Policy Definitions and Terms

### 3.9.5 Policy

The LIC, PO and PLs form the incident response team in LET, and are responsible for drafting the reporting procedures following the requirements below and in-charge of the incident response process:

1. Information on critical systems, network and data flow diagrams, hardware inventories and logging data must be constantly updated and readily available.
2. Members of the incident response team and proper incident reporting procedures must be made known to all LET Users through the LET Information Policy Training as specified in Security Awareness Policy.
3. Security logs and events from various LET Computer Equipment should be inspected and visualized actively to look out for possible incidents.

4. An IRP must be formally documented and meet the following requirements:
   (a) Proper procedure of identifying the affected Computer Equipment must be outlined.
   (b) Well-tested investigation procedures should be in place to pinpoint the root cause of the incident.
   (c) Standard way of documenting investigation process and collection of artifacts must be stated.
   (d) Appropriate evaluation systems must be specified to classify the incidents based on their impacts on LET's business goals.
   (e) Communication procedures with external organisations such as law enforcement or consultant agencies during an investigation must be defined such that minimum information related to the incident is shared.
   (f) Recovery procedures must be drafted. These must place top priority on the restoration of Computer Equipment that are essential for LET to meet its business goals.
   (g) After recovery, necessary measures must be implemented to prevent similar incidents from occurring in the future.
   (h) Damage control steps should be devised in every incident to minimise the impact on LET; i.e. reputation, financial loss and legal liabilities.
   (i) Lessons learnt must be disseminated to relevant personnel following the incident.
5. After the execution of the IRP, review meetings must be setup (with clients if applicable) to evaluate its effectiveness in handling the incident.
6. The IRP must be reviewed and tested in accordance to the *Security Audit Policy*. The IRP should be tested alongside the Disaster Recovery Plan, with simulations to assess LET's ability to respond to a significant disruption caused by a security breach. [8][11]

## 3.10 Security Audit Policy

### 3.10.1 Overview

Auditing enables an organisation to improve existing business processes as well as ensuring LET security posture is in line with the information security policies. Performing regular security audits protect the organisation's assets, data, systems and services by ensuring adequate and proper safeguards, practices and policies to minimise risks. [17][21]

### 3.10.2 Purpose

The purpose of this policy is to ensure that all of LET assets, data, systems and services are configured with compliance to LET security policies.

A security audit may be conducted to:

- Ensure confidentiality, integrity, and availability of LET sensitive information and resources.
- Investigate possible security incidents to ensure to LET security policies.
- Monitor user or system activity where appropriate, in order to ensure conformance security policies.

### 3.10.3 Scope

This policy covers all company computer systems owned or operated by LET. This policy also covers any computer system connected to the LET network which may not be owned or operated by LET.

### 3.10.4 Policy

The LIC shall have access to all computer systems owned or operated by LET to the extent necessary to perform scheduled audits that should be carried out at least once a year, as well as ad hoc audits such as after an incident or whenever deemed necessary.

1. **Guidelines**
   Approved and standardised auditing guidelines must be strictly adhered to. These guidelines include:

   (a) The compliance of all other LET information security policies must be ensured during auditing.

   (b) All computer systems must be labelled and should follow the naming convention of LET-# asset tag (e.g 13573). This is to allow easy identification of each asset during a security audit.

(c) The login image of all workstations shall be reviewed by the LIC/PO and must be updated if there are any changes.

(d) The Administrator group membership must be verified and reviewed at least once a year.

(e) Inventory information of all computing systems must be reviewed and updated accordingly.

(f) All software logs shall be sent to a central log review system to demonstrate compliance to relevant LET security policies as required, and must be retained based on the monitoring guidelines in the monitoring subsection inside the *Server Security Policy*.

(g) All audited information are deemed to be confidential and must be protected from unauthorised access or modification.

2. **Relevant Findings**

   (a) All relevant findings or deviations discovered as a result of the audit shall be listed in LET tracking system immediately in order to ensure prompt resolution or appropriate mitigating controls.

3. **Ownership of Audit Report**

   (a) All results and findings generated from the audit must be compiled into a report. This report is property of LET and classified as confidential information

## 3.11 Security Awareness Policy

### 3.11.1 Overview

LET has various information security policies in place to minimise risks that can potentially jeopardize its ability to fulfill its business goals. LET Users are supposed to act in accordance to these policies, making them the first line of defense. The Security Awareness Policy acts as the bridge for Users to learn the purposes of different polices and understand how each protects the business, Users and clients, refining Users' collective attitude towards the policies which will be better accepted and supported.

Users are often the targets of social engineering tactics and the Security Awareness Policy is critical in equipping Users with the ability to recognise and properly react to these threats in order to better protect the confidentiality, integrity and availability of LET's data.

Security Awareness policy also addresses any LET Users' privacy concerns as the different types of user activity data such as Internet activities collected, purpose behind collecting each type of data and their respective usage will be explained to Users.

### 3.11.2 Purpose

The purpose of this policy is to establish the obligations and guidelines for the dissemination of different LET information security policies to all Users. Requirements for the frequency, methodology used and evaluation of security awareness training will also be outlined in this policy. In addition, the policy serves as a deterrent for disgruntled Users claiming they were not informed about the type of data collected related to them and potential evidence to protect LET from any legal liability.

### 3.11.3 Scope

The policy applies to all LET Users.

### 3.11.4 Policy

1. **LET Information Security Policy Training** [4][7][10]

   (a) All new LET Users must attend a training session where user obligations, standard procedures, best practices, acceptable behaviours, rules, requirements and regulations under various LET information security policies will be explained as soon as practicable upon hire.

   (b) The training sessions must be conducted with a goal to induce User's acceptance and support for various information security policies by explaining their importance and how these policies protect Users and LET's business objectives, hence tempering any negative attitude arises from restrictive policies.

   (c) All new LET Users must sit for a information security policy test after the training and obtain a minimum pass. All LET Users who fail to do so must re-attend the training session until they obtain a pass.

   (d) The training on LET information security policies should then be conducted on a continuous rolling manner for all Users to maintain a reasonably consistent level of understanding of the various policies.

   (e) Updates on any LET information security policy must be promptly broadcast to all Users.

2. **Anti-Social Engineering Training** [4][7][10]

   (a) Anti-social engineering training must be conducted annually for all Users to equip them with the ability to recognise different social engineering tactics.

   (b) The training team must devise incident response procedures for different social engineering tactics following the Incident Response Procedure Guidelines as defined in the *Incident Response Policy* so that Users know how to react properly in the event of a social engineering incident.

   (c) Anti-social engineering exercises will be conducted regularly to raise awareness to evaluate the effectiveness of the anti-social engineering training. Any User who fall prey to the tactics employed during the exercise is required to re-attend the training.

3. **User Privacy Training** [4][7][10]

   (a) All new LET Users must attend a user privacy training where the different monitoring tools that LET uses for monitoring and the types of information that can be collected by these tools will be explain at a high level to Users. For example, LET emails are scanned for keywords, spam, malicious code and banned file types.

   (b) Different reports generated by the monitoring tools using the user-related data collected will be shown to Users to help them understand that their activities are being monitored to protect them and LET, rather than an invasion of their privacy.

4. **General**

   (a) The different training teams must devise training materials that suit their intended audience in terms of their styles, formats and technical level for maximised learning. For instance, non-technical Users require high level explanations.

(b) There will be a feedback channel after every training or activity to evaluate its effectiveness. The feedback, which serves as the key performance indicator of the training teams, should be taken into consideration for future training.

(c) A poster must be displayed on all Computer Equipment before the login screen to raise awareness regarding information security.

(d) Other mediums including but not limited to videos, seminars and case studies will be utilised to raise awareness about LET information security policies, social engineering tactics and user privacy.

# 4 Policy Compliance

## 4.1 Compliance Measurement

The LIC and PO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## 4.2 Exceptions

Any exception to the policy must be approved by the LIC and PO in advance.

## 4.3 Non-Compliance

Any User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.[19]

# References

[1] M. Brophy. “Sample Remote Access Policy”. In: (2015). URL: https://www.iltanet.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=5180dbb1-49ee-406e-898d-dd01145ce912&forceDialog=1 (visited on 11/22/2019).

[2] codeREADr. “Physical Security Policy”. In: (July 2018). URL: https://www.codereadr.com/compliance/physical-security-policy/ (visited on 11/15/2019).

[3] Grand Prairie Regional College. “IT Continuity, Backup and Recovery Policy”. In: (May 2016). URL: https://www.gprc.ab.ca/about/administration/policies/fetch.php?ID=319 (visited on 11/22/2019).

[4] Corporate Compliance. “Security and Privacy Awareness and Training Policy”. In: (July 2016). URL: https://community.corporatecompliance.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=dfac1d98-d41e-48d8-2f82-3a3687a6cf55 (visited on 11/22/2019).

[5] Sue Fowler. “SANS Institute: Reading Room - Auditing & Assessment”. In: (2003). URL: https://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846 (visited on 11/24/2019).

[6] “Information Classification Policy”. In: *Iso27001security.com* (). URL: https://www.iso27001security.com/ISO27k_Model_policy_on_information_classification.pdf (visited on 11/24/2019).

[7] Michelle Johnston. “Security Awareness Training and Privacy”. In: (2019). URL: https://www.sans.org/reading-room/whitepapers/awareness/security-awareness-training-privacy-394 (visited on 11/22/2019).

[8] Rasa Juzenaite. “How to Draft an Incident Response Policy”. In: (2016). URL: https://resources.infosecinstitute.com/category/certifications-training/csih-certification/creating-an-incident-response-plan/ (visited on 11/26/2019).

[9] LSE. “Access Control Policy”. In: (Nov. 2018). URL: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/accConPol.pdf (visited on 11/15/2019).

[10] IsecT Ltd. “Information Security Awareness and Training”. In: (2018). URL: https://www.iso27001security.com/ISO27k_Model_policy_on_security_awareness_and_training.pdf (visited on 11/22/2019).

[11] Carnegie Mellon. “Computer Security Incident Response Plan”. In: (Feb. 2015). URL: https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf (visited on 11/26/2019).

[12] "PHYSICAL SECURITY & ENVIRONMENTAL SECURITY". In: (). URL: https://cdn.shopify.com/s/files/1/0235/0907/files/Physical_Security_Environmental_Security_Policy_and_Procedures.pdf (visited on 11/23/2019).

[13] SANS. "Acceptable Use Policy". In: (June 2014). URL: https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy (visited on 11/24/2019).

[14] SANS. *Glossary of Security Terms*. URL: https://www.sans.org/security-resources/glossary-of-terms/ (visited on 11/21/2019).

[15] SANS. "Password Protection Policy". In: (Oct. 2017). URL: https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy (visited on 11/14/2019).

[16] SANS. "Remote Access Policy". In: (June 2014). URL: https://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy (visited on 11/22/2019).

[17] SANS. "Server Audit Policy (Retired.)" In: (Dec. 2013). URL: https://www.sans.org/security-resources/policies/retired/pdf/server-audit-policy (visited on 11/19/2019).

[18] SANS. "Server Security Policy". In: (June 2014). URL: https://www.sans.org/security-resources/policies/server-security/pdf/server-security-policy (visited on 11/22/2019).

[19] SANS. "Software Installation Policy". In: (June 2014). URL: https://www.sans.org/security-resources/policies/server-security/pdf/software-installation-policy (visited on 11/14/2019).

[20] JOSH SUMMERS. "Top VPN Protocols Explained (and which you should use)". In: (Nov. 2019). URL: https://www.allthingssecured.com/vpn/faq/vpn-protocol-guide/ (visited on 11/22/2019).

[21] Murray State University. "Audit Policy". In: (Feb. 2011). URL: https://sites.google.com/a/murraystate.edu/information-security/policy/audit (visited on 11/18/2019).

[22] Luke Voigt. "Preparing a Cybersecurity Incident Response Plan: Your Essential Checklist". In: (July 2018). URL: https://www.exabeam.com/incident-response/cybersecurity-incident-response-plan/ (visited on 11/26/2019).

[23] Vissarion Yfantis. "What Is Remote Access Control?" In: (Sept. 2018). URL: https://www.parallels.com/blogs/ras/remote-access-control/ (visited on 11/22/2019).