IT Services – Information Security Policy

Version Number:	1.2
Document Status:	Approved
Date Approved:	8th November 2021
Approved By:	Consultant Engineer
Effective Date:	8th November 2021
Date of Next Review:	7th November 2022

Table of Contents

1. Purpose and Scope

1.1. The Information Security Policy (the "Policy") sets out the approach to information security management. The Policy is in place to facilitate the protection of the Client's information and technology services against compromise of its confidentiality, integrity and availability. Whilst doing this, it recognises the ability to discover, develop and share knowledge must be maintained.

1.2. This Policy advocates a holistic approach to information security and risk. This is achieved by identifying and assessing information security threats and developing and implementing a combination of people, process and technology controls to mitigate information security risks according to a defined level of risk and the desired objectives as agreed between the client and Yellowgrid Ltd ("IT Provider"). This Policy is owned, managed and developed by the senior consultant engineers at Yellowgrid Ltd.

1.3. This Policy and the Framework applies to:

Everyone who accesses Client information assets or technology. This includes user, students and third parties.

Technologies or services used to access or process Client information assets.

Information assets processed in relation to any Client function, including by, for, or with, external parties.

Information assets that are stored by the Client or an external service provider on behalf of the Client.

Information that is transferred from and/or to the Client for a functional purpose.

3rd party, public, civic or other information that the Client is storing, curating or using on behalf of another party.

Internal and/or external processes that are used to process, transfer or store The Client information.

2. Objectives

This Policy is designed to:

Promote a holistic approach to information security management.

Protect the Client's information and technology against compromise of confidentiality, integrity (including non-repudiation2) and availability.

Support the Client's strategic vision through an approach which effectively balances usability and security.

Facilitate a 'security aware' culture across the Client and promote that Information Security is everyone's responsibility.

Protect the Client's information assets by identifying, managing and mitigating information security threats and risks.

Define security controls that are effective, sustainable and measurable.

Assist in the compliance of contractual, legal or regulatory obligations.

Identify, contain, remediate and investigate information security incidents to maintain and assist in improving the Client's information security posture.

Develop an informed approach, with regard to information security, in their daily activities across all areas of the Client, including staff (full / part time / temporary), volunteers or student staff.

Provide assurance to other parties that we have a robust control environment in place to protect their data through an effective information security management system.

3. Process and Requirements

3.1 Areas of Risk

The listing below identifies the risks the Client may be subjected to:

Virus, ransomware and malware attacks.

Emailing personal identifiable/business critical information.

Laptops – are the most common form of mobile device holding mobile data. A laptop that does not have any form of encryption can allow unauthorised access to the data contained on it.

USB memory sticks and USB connected hard drives or similar – these drives have the potential to store large quantities of data are easily lost and misappropriated.

Desktop PCs – should be risk assessed and those identified at risk must be encrypted with full disk encryption. It is policy that data should not be stored on the local hard drive so it would only be desktops which have a valid business reason to store data locally and are in vulnerable locations that would require encrypting.

Other mobile devices – including PDA's, smart phones, CD, iPhones, iPad, DVD's, etc… The loss of any of these devices containing sensitive data would compromise the Client's information security if there was not robust encryption in place.

3.2 Virus and Malware Protection

Up to date anti-virus software for the detecting, removing and protecting against suspected viruses shall be installed on all servers, workstations, and laptops.

Anti-virus software shall be updated regularly for all servers, workstations and laptops with the latest anti-virus patches and/or signatures, where applicable.

Heuristic anti-virus software (signatureless) and zero-day threat analysis / protection is used.

Users shall be made aware of current anti-virus procedures and policies.

Personnel shall inform the IT provider immediately in the event of a possible virus infection.

Upon notification of a virus infection systems shall be isolated from the network, scanned, and cleaned appropriately. Any removable media or other systems to which the virus shall have spread shall be treated accordingly.

If a system has been identified as potentially infected and removal/quarantine of the virus/malware cannot be definitively proven, the system shall be completely wiped and re-imaged.

3.3 Encryption Strategy

Laptops: All Client laptops must be encrypted with BitLocker full disk encryption with AES encryption algorithm and a 256-bit key is used. Laptops are encrypted by the ICT provider, prior to being distributed to staff.

USB memory sticks and USB connected hard drives: Individuals wishing to use removeable USB memory sticks or hard drives should use full disk encryption with AES encryption algorithm and a 256-bit key, such as Bitlocker or OS equivalent tool.
Mobile devices can be connected to the Client email system. PIN lock access codes are enforced before the device connects to the email server. Enabling an access PIN code ensures the data on the device is encrypted. Remote wipe is enabled in the event of device loss.

3.4. Backup Policy

Daily backups of data, applications, and the configuration of servers and supporting devices shall occur to enable data recovery in the event of a disaster or business continuity event.
All backups shall be encrypted for data at rest and in transit.
Backups shall be encrypted and stored in a physically and logically secure geographically separate location.
Backups are monitored using an RMM solution and success and failure alerts are generated and acted upon accordingly

3.5 Password Policy

Minimum of seven (7) characters in length. Passwords should include at least a variation of three out of the four categories below:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic complex characters (e.g., !, $, #, %).
Passwords history shall be kept for the previous twenty four (24) passwords and passwords shall be unique across the password history.
Maximum password age should be one hundred and twenty (120) days.
Shall not be the same as or include the user id.
Passwords shall not be easily guessable.
Set first-time passwords to a unique value for each user and change immediately after the first use.
User accounts shall be locked after five (5) incorrect attempts. Lockout duration shall be set to a minimum of thirty (30) minutes or until an administrator resets the user's ID upon proper user identify verification.
If a session has been idle for more than ten (10) minutes, the user shall be required to re-enter the password to re-activate access.
Password hints should not be used.

The following shall be adhered to when managing user passwords:

Verify user identity before performing password resets.
Where possible, these requirements shall be automatically enforced using management tools such as Active Directory Group Policy or specific system configuration(s).
Role based access to all systems shall be implemented, including individually assigned username and passwords.

Usernames and passwords shall not be shared, written down or stored in easily accessible areas.
Group, shared, or generic accounts and passwords shall not be used unless approved by Information Security (e.g., service accounts) and shall follow approved information security standards.
Special administrative accounts, such as root, shall implement additional controls, such as alerting, to detect and/or prevent unauthorized usage.
Administrator, superuser, and service account passwords shall be stored in a secure location or electronic password safe
Default passwords on systems must be changed after installation.
Mandatory password changes should occur if a password breach is identified, or the user suspects their password may have been compromised.

3.6 Authorized Software Policy
Only authorized, supported, and properly licensed software shall only be installed on Client owned or managed systems.
Only IT administrators or specific personnel who have been granted administrator access shall install authorized and licensed software.
The use of unauthorized software is prohibited. Immediate removal of unauthorized software is required if discovered.
Workstation configurations or build standards defined by the IT provider in alignment with Information Security policies are required to be followed. Change of definitions is only allowed by the IT provider, or authorized parties who have been specifically granted administrator access.
A security review and approval of all software shall be completed prior to production release. The review shall be based on system criticality and data type. Free, shareware, and open-source software as well as software as a service (SaaS) shall be reviewed as well.

3.7. Server Security Policy
Servers shall be physically secured.
Access via unencrypted protocols (i.e Telnet / FTP) is not allowed without prior Information Security approval.
Server administrators shall be limited to one primary administrator and backup administrators, where feasible.
All servers are required to use universal power supplies (UPS).
UPS software shall be installed on all servers to implement an orderly shutdown in the event of a total power failure. All UPSs shall be periodically tested.
Servers are monitored using an RMM solution for hardware failures using SNMP.

3.8. Mobile & Remote Computing Policy
Ensure appropriate controls are in place to mitigate risks to protected information from mobile computing and remote working environments.

Use of personally owned devices shall comply to acceptable use and information security policies if used to access Personal Data, PII or SCI data.
Devices owned by personnel shall never be used to access customer data, unless appropriate monitored controls, approved by Information Security, have been implemented.
Devices owned by personnel or authorized parties are not allowed to connect to corporate or production networks.

3.9. Network Security Policy
Access to internal and external network services shall be controlled through:
Network access control lists (NACLs), or equivalent.
Firewall policies, or equivalent.
Security groups, or equivalent.
IP whitelists, or equivalent.
Gateway security services; antivirus, intrusion prevention services, traffic analysis is used to prevent threats from entering the network at the perimeter.
A multi-tier architecture that prevents direct access to data stores from the internet.
Usage of role-based access controls (RBAC) shall be implemented to ensure appropriate access to networks.
Two-factor authentication shall be implemented where possible.
Firewalls, routers, and access control lists, or equivalent access controls, shall be used to regulate network traffic for connections to/from the Internet or other external networks, as follows:
Configuration standards shall be established and implemented.
Access control policy shall limit inbound and outbound traffic to only necessary protocols, ports, and/or destinations.
Internal IP address ranges shall be restricted from passing from the Internet into the DMZ or internal networks.
LAN equipment, hubs, bridges, repeaters, routers and switches shall be kept in physically secured facilities.
Network equipment access shall be restricted to appropriate personnel only. Other staff and contractors requiring access are required to be supervised.
Network cabling shall be documented in physical and/or logical network diagrams.

3.10. Wireless Network Security Policy
Wireless networks shall be encrypted
Access to wireless networks shall be restricted to only authorized devices. Any SSID can be used as long at the appropriate device and access and authentication types are utilised.
Wireless network configuration should be as follows:

<u>Corporate Owned:</u>
Network Access: All corporate plus Internet
<u>Guest BYOD:</u>
Network Access: Only Internet
Any wireless network encryption requirements that cannot be addressed by the identified

device types above must be reviewed and approved by Information Security.
Personnel and authorized third parties are not allowed to install unauthorized wireless equipment.
Default SSIDs and usernames and passwords shall be modified or removed prior to implementation in a production environment.

3.11. Messaging Security Policy
All incoming email shall be scanned for viruses, phishing attempts, and spam.

3.12. Removable Media Policy

Using removable media should be avoided wherever possible.
All removable media brought in from outside the Client network should be scanned for viruses/malware prior to use. Any identified malware/viruses shall be removed with the assistance of End User Support prior to use.
In the rare event that physical media needs to be used, the applicable details, including the type of physical media, the authorized sender/recipients, the date and time, the number of physical media, and the type of encryption used should be documented.

4. Training
4.1 To maintain adequate levels of knowledge and awareness of IT security and cyber threats Clients are encouraged to have staff and users access online material and training which is provided free by NCSC https://www.ncsc.gov.uk