Policies and Procedures

Operations Department

IT Security Policy and Procedure

Policy Author	Katya Galea	**Designation**	
Policy Reviewer	Rosanne Galea	**Designation**	Managing Director
Policy Approver	QAC	**Revised Date**	26/07/2024

IT Security Policy and Procedure

1. Applicability

This policy and procedure is applicable to all Staff and Students.

2. Introduction

It is the policy of Future Focus ("the Institution") to prohibit unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of information and equipment.

The Institution is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic information assets and equipment to ensure that legal, regulatory, operational and contractual requirements are fulfilled.

The Institution wishes to support its staff and students in using IT and information systems safely and securely, in addition, cybercrime poses a real and growing threat for the Institution, and it is not something that should be ignored. Preventing both internal and external threats, the Institution recognises that the ability to protect systems and data is a fundamental enabler for the Institution's wider strategy. Promoting an effective security culture will therefore be beneficial to both the institution and the individuals within it.

This policy is owned by the Institution and reviewed by the Institution accordingly.

3. Purpose

This security policy is intended to ensure the confidentiality, integrity and availability of data and resources through the use of effective and established IT security processes and procedures.

4. The Policy

Section A: Definition

This security policy is intended to ensure the confidentiality, integrity and availability of data and resources through the use of effective and established IT security processes and procedures.

Section B: Responsibilities

The HOI is responsible for reviewing and approving information security policy and responsibilities, reviewing and monitoring security incidents and approving major initiatives to enhance information security.

The Future Focus IT Service Provider is responsible for managing information security within the Institution. This includes implementing and supporting the Institution's wide security initiatives, developing contacts with internal and external security specialists, keeping up with industrial trends, monitoring standards and advising on security issues. In addition to conducting investigations into any alleged computer or network security compromises, incidents and/or problems.

Institution programme leaders and executives must ensure that staff within their management control area are made aware of this and other relating policies and security mechanisms. Executives and leaders must make all efforts to incorporate security procedures into staff briefings and training programs. Where applicable ensure computer and communication system security measures are observed.

Executives and leaders must report promptly all significant changes in User duties or employment status to the local administrators responsible for user accounts. In addition, executives and leaders are expected to ensure their staff receive appropriate training and guidance to manage information security.

Individual users of Future Focus IT equipment are expected to have some basic computer knowledge and should understand and adhere to Institution security policies and procedures. Users must protect against the misuse of computer system accounts issued to them, select and maintain good passwords and provide the correct identity and authentication information when requested. Standard facilities should be used for securing access to their workstation when left unattended, users must also notify the helpline or line management if a security violation or failure is observed or suspected. Users must not exploit system weaknesses or attempt to assume another party's identity.

Service administrators are expected to support and enforce applicable security policies and procedures including managing all user access privileges to data, programs and functions.

Maintain and protect server software using available and approved security mechanisms. Monitor all security related events and following up on any actual or suspected violations where appropriate and report in line with section H of this policy.

IT service providers are responsible for enforcing Institution security policies as they relate to technical controls in hardware and software. This includes developing appropriate procedures and issuing instructions for the prevention, detection and removal of malicious software. All data and software should be backed up on the systems/networks on a timely basis and critical programs and data archived if applicable. Network administrators should also ensure the network environment within the site and interfaces to outside networks are secure, control access to and protect network physical facilities, conduct timely audits and monitoring of server logs, incident logs and reports and report where applicable. Emergency events must be responded to in a timely and effective manner and the Information Security Manager promptly notified of all computer security incidents.

Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) are expected to comply with this IT Security Policy regarding their designated systems specifically Section E.

Contractual partners and contracted consultants must abide by Future Focus's policies and procedures including the Acceptable Use Policy prior to accessing Institution systems and services. The IT System owner is responsible for ensuring that this is implemented.

External Service Providers must abide by Future Focus's policies and procedures when accessing Institution systems and services or data. The System owner is responsible for ensuring that this is implemented. Consultation with External Service Providers must be done in conjunction with the External Service Provider policy.

Section C: Physical and Environmental Security

All Institution network equipment must be physically secured with appropriate access control in place to ensure that only authorised personnel have access. Local area servers must be placed in locked cabinets in areas of public access or locked computer rooms.

Wherever practical as determined by IT Services; equipment must be sited in a suitable environment to prevent loss, damage, or compromise of service and interruption to business activities.

The IT service provider is responsible for approving physical access to Institution Data Centres.

All persons accessing Institution IT areas should be prepared to produce Institution or third-party ID cards on demand, ID's cards must not be transferred to a third party or to colleagues. Visitors must be escorted in secure areas if applicable.

All external doors and windows must be closed and locked at the end of the workday.

Controls should be adopted to minimise the risk or potential threats to the physical equipment including theft, fire, dust, liquid damage, electrical interference or failure, chemical effects or environmental hazards.

Users are responsible for ensuring the security of their own belongings and for the IT equipment associated with the workstation they are operating from. Computers and laptops must not be left logged on when unattended and must be protected by passwords and screensavers. Screens can be locked by the user when leaving their computer terminal, however, at the end of a work session, devices must be shut down and not locked so that the device can be used by other users.

Section D: Network

This section sets out the requirements for the protection of the confidentiality, integrity and availability of the Institution network. The network for the purpose of this policy is a collection of communication equipment such as servers, computers and printers which are connected together using the Institution local and wide area network and wireless networks.

The Network is owned by the institution and administered by IT Service Provider. The security of the network is the responsibility of IT Service Provider.

The Institution network is protected by key controls such as Firewalls, Intrusion Prevention System, Mail and Web Filtering, Anti-Virus, VPN, Access Control Lists as well as further underlying security controls to prevent the network from both internal and external threats.

The IT Service Provider, will co-ordinate the delivery of an annual programme of penetration testing on areas of the network based on risk, impact and priority. Penetration testing might be conducted by an external specialist provider and/or internal audit or through use of internal expertise.

Computer and network resources must not be wilfully or negligently used to attempt to breach the security of the Institution or security of other sites. There should be an inventory containing all equipment connected to the Institution's wired networks and all access to Future Focus's networks should be logged.

Where the software allows, computer and communications systems handling sensitive, valuable, or critical Institution information must securely log all significant security events.

The connection of any major non-Institution owned IT equipment to the Institution network must be approved by IT Service Provider and carried out by suitably technically qualified support staff.

When using a device connected to the Institution network, users must log in with a username and password supplied by IT Service provider.

Computer or communications systems attached to the Institution network must include sufficient automated tools to assist the administrator in verifying the systems' security status. These tools must include mechanisms for the recording, detection, and correction of commonly encountered security problems.

Usernames and Passwords for users accessing the Institution domain or secured web pages from an external source must have security in place to protect authentication details. No Usernames and Passwords should be sent in clear text format. This would include access by wireless technology.

System users must respect the physical network configuration of Institution owned networks and must not extend the physical network on which their system resides.

Section E: Access Control

E1: Creating, Controlling and Managing User Accounts

Written procedures for access control and passwords based on business and security requirements must be in place. Password procedures should contain password requirements such as frequency of change, minimum length, character types which may or must be utilised and regulate password storage.

Users accessing systems must be authenticated according to Institution procedures. Users should have unique combinations of usernames and passwords and are responsible for any usage of their usernames and passwords. Users must keep their passwords and system passwords confidential and not disclose them.

Users should only have access to the services they are authorised for, access to information systems should be granted on a "need to know" basis and take into account access rights, associated privileges and be authorised in accordance with the system owners. Access to privileged accounts and sensitive areas should be restricted. Users should be prevented from accessing unauthorised information.

Remote access to the Institution's computer equipment and services is only permitted if the IT Security and Acceptable Use Policy has been read and understood. All remote access from external suppliers must be risk assessed and authorised by the IT Service Provider.

Remote access to the Institution's network may only take place through security solutions approved by the IT service provider.

A User is defined as:

1. A named Person who has a contract of employment with the Institution.
2. A named Student who has a current enrolment on a programme of study.
3. A named Applicant Student who has a firm or conditional offer for a programme of study.
4. A Contractual Partner, Contracted Consultant or External Service Provider where there is a legally binding contract to provide services to, or consume services from, the Institution.

Privileged Access information system accounts will only be provided to named members of the IT Service provider and only with the written (email) consent of the Future Focus leaders and executives.

Non named information system accounts will only be provided to named members of the IT Services department to support operational technology needs and only with the written (email) consent of the Future Focus IT Security Manager.

No other information systems access will be provided and no Guest or Temporary access accounts will be created.

E2: Granting and Revoking Systems Privileges

Requests for a user account, access privileges and email system access must be granted only by a clear chain of authority. Approval must be obtained from the user's line manager before a service administrator grants access privileges.

The ability to create and allow access to servers, services or applications is limited to employees with relevant authority. System and network privileges of all users, systems and programs must be restricted to the lowest level required to meet business needs. Excessive privileges granted to users must be avoided.

All user-accounts must automatically have the associated privileges revoked after a certain period of inactivity. The recommended period is one hundred and fifty (150) days.

On written (Email) application of appropriate management or Human Resources staff, user accounts and associated privileges will be suspended immediately.

All user accounts must be disabled on cessation of employment. This is to include any access to shared mailboxes which may fall outside of the user’s normal logon details.

Log-in banners on multi-user computers must include a notice stating:

- This system is to be used only by authorised users.

- Continuing to use this system requires compliance with Institution conditions of use.
- Log-in banners must have physical input to continue.

E3: Password Control

The following password measures should be implemented on all Institution systems and networks:

- All server accounts must be password protected, user account passwords may not be shared with or revealed to anyone. Where applicable different passwords should be used for different systems.
- User account passwords must not be written down and left in a place where unauthorised persons might discover them.
- Passwords should be at least 8 characters in length, contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z), have at least one numerical character (e.g. 0-9)
- All vendor supplied generic accounts and default passwords must be changed.
- Non-personal accounts must be assigned to a named person, who will be held responsible for that account and should maintain an audit trail of said account.
- No employees leaving the organisation on termination of employment should retain access to non-personal accounts, account passwords should be changed.
- Multi-user accounts and passwords must not be used unless strict password management is in place.
- System accounts and passwords should be secured and used only in emergencies.

- All passwords must be changed immediately if they are suspected of being disclosed, or known to have been disclosed to anyone. Whenever system/network security has been compromised, or even if there is a convincing reason to believe that it has been compromised, the relevant local administrator should immediately reassign all relevant passwords, and broadcast a message to all concerned telling them to change their passwords.

E4: Monitoring of System Access and Usage

Access and use of IT systems should be logged and monitored in order to detect unauthorised information processing activities. Usage and decisions should be traceable to a specific entity, e.g. a person or a specific system. The IT department should register substantial disruptions and irregularities of system operations, along with potential causes of the errors.

Capacity, uptime and quality of the IT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.

E5: External Third-Party Access to Institution Assets

External parties include customers, consultants, auditors, developers and suppliers. Assets include information (databases, data files, etc.), software, hardware (including removable media) and services.

No third-party IT must be installed on Future Focus's corporate network without explicit consent from the IT service provider. Access to the Institution network, servers, or information systems by third parties must be controlled. Access requirements of any third party will be risk assessed by the IT service provider. Access will not be granted until the successful outcome of an assessment.

Access provided to third party organisations must have formal agreements or contracts in place.

Third party accounts must be configured to automatically disable after the period defined in the contract.

Section F: Safeguarding Data, Backup and Encryption

F1: Safeguarding Data

Users of Institution desktop PCs where possible should always save data to their cloud share (OneDrive). Users are not encouraged to saved data to the local PC hard disk where no back up may exist and hard disk failure may occur.

All Institution servers must be served by or fitted with a suitable back up device.

Users must only be added to the workstation administrators group if authority has been granted by the IT Services department or IT Security Manager.

Institution PC's should not be used to host business critical services, where possible services should be deployed to servers and data backed up to network shares.

Changes to network configuration (IP number, Machine name etc.) must only be carried out by IT Services technical staff.

Local PC administrator accounts must not be disclosed to users. Changes to PC administrator accounts must only be carried out by authorised IT service provider staff.

No data or information intended for employees only should be stored on personal email accounts of personal devices.

IT Services must ensure the documentation of physical and virtual servers, services hosted, protocol usage and available ports must be in the possession of relevant core administrators.

Firewall technology must be made available and utilised on systems identified as requiring such a level of security.

All computers, IT devices and servers connected to the Institution network where applicable must run a version of the Operating System and installed applications with the latest available security patches and updates, all computers and servers must have approved and up to date virus-scanning software enabled. No exceptions should be placed in antivirus software without consent from IT Services. Users must notify IT Services immediately if they suspect their PC has become infected. Any PC service or system suspected of being infected must be isolated from the network immediately.

Appropriate technical and organisational controls for physically securing media including but not limited to computers, removable electronic media, receipts, paper reports, and faxes to prevent unauthorised persons from gaining access to personal data, cardholder data or organisationally sensitive data must be in place.

F2: Backups and Recovery

Specialist computer staff will install or provide technical assistance for the installation of backup hardware and/or software. Ensuring adequate controls and procedures are in place for the backup of Institution data is the responsibility of the IT service provider and the systems administrator involved in the back-up process.

All sensitive or confidential, valuable, or critical information resident on Institution computer systems and networks must be regularly backed-up.

Data Owners should define which information and which machines are to be backed-up, the frequency of back-up, and the method of back-up.

Where possible backup procedures should be automated and not require manual processes.

If the system supports more than one individual and contains data that is critical to the day- today operation within the Institution, then back-up is required daily.

Back-ups for critical business functions should be stored off-site in suitable secure conditions.

Back-up and recovery procedures must be documented by the IT service provider.

F3: Encryption

Storage and transfer of sensitive information (organisational sensitive data or personal data defined by the relevant data protection legislation) should be encrypted or password protected.

Section G: System Acquisition, Planning and Maintenance

G1: Operational Procedures and Areas of Responsibility

Purchase and installation of IT equipment or software must be approved by the IT

Service provider. The IT Service provider must ensure where possible the installation of new equipment and software is done in accordance with the manufacturer's security guidance.

Changes to IT systems, equipment or software must be authorised by the Director or Head of Operations.

Operational procedures should be documented for new systems, services and software or where changes have been made

Implementation of all new IT systems should be formally risk assessed. Before a new IT system is put into production, plans and risk assessments should be in place to avoid errors or identify unforeseen issues. Information Security should be incorporated into the Project lifecycle of all new system or software implementation.

Duties and responsibilities should be separated where possible to reduce the possibility of unauthorised or unforeseen abuse of Future Focus's IT equipment and services.

The IT Services provider must ensure development, testing and maintenance environments are separated from operational IT environments to reduce the risk of unauthorised access or changes, and in order to reduce the risk of impact following error conditions.

G2: System Planning and Acceptance

Requirements for information security must be taken into consideration when designing, testing, implementing and upgrading IT systems, as well as during system changes. Routines must be developed for change management and system development/maintenance.

IT systems must be designed according to scalability and cost requirements. The load should be monitored by IT services in order to apply upgrades and adjustments in a timely manner. This is especially important for business-critical systems.

G3: Applications and Services

Operating systems must be approved by the IT service provider.

Users shall only use legally obtained software on Institution computing equipment. The unauthorised use of hardware or software, which interrogates the network in any way, is forbidden.

It remains the responsibility of the user to ensure that they do not infringe copyright in their use of software provided to them by the Institution.

Section H: Information Security Incident Management

Actual or potential computer security compromises including lost or stolen devices containing Future Focus data including personal devices used for business reasons such as email must be reported to the IT Security Service Provider. For lost and stolen PC equipment a notification to the police may be necessary.

All staff, students and third parties must report promptly any suspected information security incident including intrusions and out-of-compliance situations.

All staff, students and third parties are required to report to computer virus notifications to the Institution helpline immediately.

All network or systems software malfunctions must be reported to the Institution IT service provider.

Section I: Website and content filtering

The Institution exercise its right to use firewall and web filtering technologies to prevent access to undesirable web sites through the external web filter provider allows for the application of automatic site blocking by a range of categories i.e. 'Adult', 'Hacking', 'Racism', the list of which is maintained by the web filtering software supplier, not Future Focus.

Section J: Policy Enforcement, Review and Update

J1: Enforcement

Institution staff must be notified that this policy exists and that they are expected to comply with the policy.

Compliance with security policies is for the protection of all concerned.

Failure to comply with this policy will expose Institution information and systems to unacceptable risk.

Under rare circumstances, certain persons will need to employ systems that are not compliant with this policy. All instances must be approved in advance by the Director

Failure to comply with Institution security policy may lead to disciplinary action being taken.

Further guidance may be obtained from Director or Head of Operations.

5. Roles and Responsibilities

This policy is applicable to, and will be communicated to, all Future Focus employees, students, third parties who interact with information held by the Institution whether processed on site or externally and the information systems used to store it.