POLICY:		ICT SECURITY POLICY
FIRST DRAFT:		ET 2015#11 (21 October 2015)
ADOPTED:		BR 2016#01 (16 March 2016)
AMENDMENTS:		
REVIEW:		March 2021

Contents

1.0 Review

The Security policy is reviewed annually. This is scheduled in TrackIT. All policies, guidelines and protocols of Mary Immaculate College, will reflect the Colleges commitment to the promotion of equality and will be fully compliant with the provisions of prevailing equality legislation.

2.0 Goal of MIC Security policy

Protect the college's physical ICT assets and data from accidental or malicious disclosure, modification, or destruction.

3.0 Scope

- This policy includes access to MIC computing spaces as managed by ICT Services, such as server rooms, lab rooms.
- This policy applies to all MIC-owned computing and communication equipment, such as servers, desktops, laptops and other mobile devices.
- This policy applies to the MIC network and connected networks and to all equipment connected to those networks physically or via wireless.
- This policy applies to all college staff, students, third party providers and users of MIC ICT assets and network including resources provided through the MIC wired and wireless networks.

4.0 Risk Statement

This policy mitigates the risk of a security incident occurring.

5.0 ICT Assets including Mobile Devices

- ICT Equipment should not be purchased without prior consultation with ICT Services.
- All ICT assets must be registered with ICT Services and recorded in the ICT Asset Database.
- A log of the location of all ICT Assets is maintained in this Database.
- The College and all of its employees are obligated to protect corporate data and ICT Assets. If data or assets become compromised or threatened due to the loss or theft of ICT equipment, the College and its employees must immediately take steps to prevent

or minimize the harm or damage that could result. This involves contacting the Data Compliance Office and ICT Helpdesk immediately to report any incidents.

- All ICT equipment is stored in the Res Block ICT Store and ICT areas when not in use.
- The physical security of mobile devices is the responsibility of the person who has a mobile device in their possession and all reasonable precautions should be taken to protect such devices from damage and theft.
- All Mobile devices must be encrypted and password protected.
- Only connect mobile devices to secured Wi-Fi networks when off-campus.
- Regularly update the software on mobile devices while observing advisory notices issued by ICT Services.

5.1 Asset Disposal

The College must implement the physical disposal of technology assets no longer in use. There are two primary methods of disposal:

1. Transfer of Ownership/Donation – Donating non-hazardous, functioning technology to registered non-profit organizations should be considered on a case-by-case basis. Any such arrangements must adhere to manufacturers' end-user license agreements and applicable copyright laws. Approval for all donations—hardware and software—should be authorized by ICT Management. ICT assets donated to organisations must be more than 4 years old.
2. Recycling – ICT Assets not disposed of under section 1 above, should be physically disposed of in accordance with Waste Electronic and Electrical Equipment (WEEE) regulation. The physical disposal should be undertaken by certified or licensed e-waste professionals.

All data must be wiped from ICT Assets prior to disposal. In addition, the disposal must be recorded in the ICT Asset Database. All documentation, such as certificate of destruction, bill of sale, and receipt by an e-waste recycling facility should be saved to Asset Destruction Folder.

6.0 Access

6.1 Physical Access

- Access to server rooms are controlled by the Salto lock security system. Only authorised users approved by ICT Management can gain access.
- Server rooms are alarmed and the alarm must be set on exiting the Server room.
- Contractors / Vendors must be authorised by an ICT member and then complete the room access log to gain access to a server room.

6.2 Network Access Controls

- Access to College network and facilities is restricted to authorised College users. Users are required to login to an authorised domain using a secure username/password combination. Additional authentication mechanisms may be required if ICT Services deem it necessary.
- Obsolete Student domain accounts are removed once every semester as per the records in the Student Records system.
- Staff domain accounts are managed as per the Starters and Leavers Policy.
- MIC Staff who retire are allowed to retain their network account.
- All equipment connected to the College network must conform to the appropriate standards as set periodically by ICT Services and run only protocols supported by the College.
- Equipment should not be physically connected to the college network without prior approval by ICT Services.
- Connection to wireless network services requires authentication.
- A scan of open file shares will be performed annually.
- A penetration test will be performed on the DMZ bi-annually using the Nessus product which is made available through HEAnet.

6.3 Password Controls

The following controls apply to user domain account passwords:

- A valid password must consist of at least 8 characters and must comply to 3 of the 4 complexity rules:
    1. Password contains English uppercase character(s) (A to Z)
    2. Password contains English lowercase character(s) (a to z)
    3. Password contains Numeral(s) (0 to 9)
    4. Password contains non alphabetic character(s) (i.e. # $ % !)
- Passwords maximum age is 90 days, and the user will be prompted to change at this time. In certain circumstances (e.g. service accounts) passwords are set to never expire where authorised by ICT Management.
- Password history maintains a history of the last 3 passwords.
- If an account or password is suspected to have been compromised, report the incident to the ICT Helpdesk immediately.
- Whenever an unauthorised party has compromised a system, the ICT Services Department must immediately change every password on the involved system. Even suspicion of a compromise likewise requires that all passwords be changed immediately.
- All vendor-supplied default passwords e.g. default passwords supplied with routers, switches or software such as operating systems and databases must be changed before any computer or communications system is used.
- The identity of any user who contact ICT Services to reset their password needs to have their identity verified either by producing an ID Card or else be known to the ICT Help Desk staff member.

6.4 Connection of Privately Owned Equipment

- Authorised Network users may only connect privately owned computing equipment to the college wireless network.
- If there is any suspicion that ICT equipment may be infected or compromised in any way it should not be connected without prior consultation with ICT Services.

7.0 Use of Network Facilities

- All data, programs or devices created, owned or stored by a user on or connected to college network facilities may be subject to inspection by the ICT Services Director or nominee in the instance of suspected wrongdoing.
- A user shall be required to provide the decryption key to facilitate decryption of data/programs where data or programs are encrypted. MIC management reserves the right to remove/delete any programs or data.

8.0 Software

- Academic users are made administrators on client computers.
- Other users may be administrators on local pcs where deemed necessary by ICT Services.
- Only licensed authorised software may be used on ICT equipment or on the ICT network.
- ICT Services should be consulted prior to installing any software.
- Users should not download, install or use unauthorised software programs.
- Software packages that permit the computer to be 'remote controlled' and 'hacking tools' are explicitly forbidden on MIC equipment unless they have been explicitly pre-authorised by management for legitimate business purposes.
- The ICT Department implements antivirus on windows domain client computers.

8.1 Patch Management

- The ICT Services Department are responsible for applying security patches to Microsoft products via WSUS.
- The ICT Services Department is also responsible for monitoring any newly discovered vulnerabilities and assessing if action needs to be taken to protect the MIC network.

9.0 Email

- The College employs anti-spam software (currently MailMarshal) to check, segregate and quarantine unsolicited commercial mail.
- Incoming and outgoing e-mails are virus-checked.

- Use of College E-mail for occasional, personal, non-commercial purposes is acceptable provided that it does not interfere with the business of the College or contravene any college policies.
- Users can delegate access to other users and this access is under the control of each individual user.
- When delegated access is granted centrally following a request then a report on this granted access is sent to the individual every 6 months. The user is required to verify that they are satisfied with this access or contact the ICT Helpdesk with instructions on changes that need to be made.
- The College reserves the right to review, audit, intercept, access and disclose messages created, received or sent in certain circumstances, including where:
    - There is reason to suspect that this Policy and/or any other college policy is being breached;
    - For the purposes of back-up and/or problem solving;
    - When MIC is required to do so by law;
    - Where, without access to the information in the account, the operations or functions of the College or a College department are likely to be seriously obstructed or impeded or where there could be serious safety or financial implications;
    - Where the account holder is no longer a member of staff ;
    - Where information in required in relation to Freedom of information request.
- When an e-mail message is undeliverable (this is normally due to an incorrect address in which case the e-mail is redirected to the e-mail administrator who has to either open or redirect it accordingly or discard it).

10.0 Data Protection

It is the responsibility of each member of staff to be diligent in fulfilling obligations in relation to data protection. This includes saving data that is considered sensitive in nature and not considered public information on public cloud offering that do not meet the standards of ICT

Services. If in doubt consult ICT Services. The list of services not approved for sensitive data storage include iCloud, Google Drive and DropBox.

11.0 Remote Access Connection

Remote access connection to the College network is allowed to all senior management and to users where a valid business reason exists with department manager approval. The college currently provision VPN access using the facility available on the firewall. All VPN Users will be reviewed annually to ensure such access is justified.

Third Party vendors may be granted access to the college network for the purposes of providing support. Approval needs to be provided by ICT management and access should limited to required systems and for a restricted timeframe.

12.0 Security Incidents/Misuse

All ICT related security incidents/policy breach must be reported to the Data Compliance Office and the ICT helpdesk immediately.

13.0 Supporting Policies

The following policies and guidelines specifically but not exclusively complement and support the MIC Security Policy.

1. Credit Card Security Policy
2. Responsible Computing Policy
3. Data Protection Policy
4. Starters and Leavers Policy