TITLE: ***INFORMATION SECURITY POLICY***

Effective Date	06 February 2019	**Version**	01
Approved By	Management Board	**Date Approved**	06 February 2019
		Review Date	06 February 2022 *or as required*
Superseded or Obsolete Policy / Procedure(s)		**Owner**	
		IT Services	

1. Purpose of Policy

Carlow College, St. Patrick's (hereafter Carlow College) is committed to providing a secure platform for management, storage and processing of information. Information is a critical asset to the College which highlights the integral role of security for the technological platform on which the information is located within the College, to ensure business continuity, compliance and prevent financial loss to the College. The vast increase in cybercrime has caused further requirement for vigilance on network security to ensure integrity, confidentiality and availability of information within Carlow College.

The purpose of this Policy is to protect Carlow College's technological network infrastructure and information stored within from internal, external, accidental and deliberate threat to security. The policy, along with associated documentation, will define security controls necessary to safeguard information systems from security breaches.

2. Definitions

Confidentiality **–** Only authorised access to data

Data User – a person who controls, holds, processes and uses data as part of their role

Information processing – performing operations such as:

- Obtaining, recording and retention of information
- Organising, storage, editing or adaption of information
- Retrieving or accessing information

- Communication or disclosure of information through electronic transmission
- Deletion or discarding of information

Information Security – ISO27002 defines information security as ensuring confidentiality, availability and integrity of information.

Information Technology (IT) Infrastructure – includes all computer devices, applications, services, network resources and communication equipment. This also includes email/internet facilities, network logon and information owned by CCSP.

Risk – an event which can have consequences on economic performance and professional reputation.

Security Breach – unauthorised access to information, applications, networks or services which bypasses existing security measures.

3. Scope of Policy

This Policy applies to all Carlow College staff, learners, contractors, agency staff and authorised third-party service providers that use the IT infrastructure within the College and process information on behalf of the College. This Policy takes precedence over any other policies which may be developed at local level.

4. Policy Statement

Carlow College recognises their responsibility and the underlying principles to ensure best practice for the protection, management and security of data, through identifying and mitigating risk to critical assets of the College. The objective of the *Information Security Policy* is to outline and implement effective technological and operation security controls to preserver the availability, confidentiality and integrity of all college data. This Policy will identify best practice in line with industry recommendations which should be followed by all data users in the College. Means by which the objectives of this Policy will be reached include:

- monitoring and auditing of all activity on CCSP network including logs and network traffic;
- identifying, managing and mitigating risk to information systems through regular risk assessment; and
- ongoing auditing and improvement of security controls including user awareness and updating of policies and recommended guidelines.

Information Security Guidelines (Appendix 1), outline the measures which will be put in place to achieve the objectives of this Policy.

4.1: Security Breach

To preserve the confidentiality, availability and integrity of all CCSP data, IT Services reserves the right to record all network activity and logs to identify vulnerabilities to the network and mitigate risk.

All suspected breaches of data security must be reported to Data Protection Officer or IT Services immediately. IT Services will then advise on next steps depending on the nature of the security breach and level of risk identified.

Breach of security or contravention of the policy, this may result in disciplinary action.

5. Responsibilities

5.1: IT Officer

The IT Officer is responsible for:

- developing and publishing the Policy;
- amending and reviewing the Policy;
- the identification and implementation of suitable security control necessary to protect and safeguard Carlow College network and the data stored;
- the backup of all college data stored on the Carlow College network (excluding files stored on local hard drives); and
- the implementation of appropriate access management controls.

5.2: IT Services

IT Services is responsible for facilitating the following information security principles:

- confidentiality of data;
- availability of data; and
- integrity of data.

5.3: Line Managers

Line Managers are responsible for:

- ensuring that the activities undertaken within the relevant department / function are carried out in a safe manner without undue risk to the health and safety of College employees, learners or any third parties. This duty extends to home / remote workers;
- the implementation of this Policy within the area for which they are responsible; and
- consulting with the Data Protection Officer or IT Services to ensure appropriate procedures are followed in the event of a breach to information security.

5.4: Data Owners

The data owner is accountable for data assets in their area and authorises use of that data. Data owners must adhere to *Records Management Policy* and *Data Protection Policy*, along with all associated documentation, to ensure relevant measures are in place to protect the data for which they own.

5.5: Data Users

Data Users are responsible for:

- complying with this Policy and all other data related policies and guidelines outlined in associated documentation;
- using best practice to protect information ensuring confidentiality, availability and integrity of data;

- reporting of any suspected breach of information security in line with Personal Data Breach Response Plan. All suspected information security breaches must be reported to the Data Protection Officer.

6. Associated Documentation

- Appendix 1: Information Security Guidelines

Please note that the associated documentation of the 'Referenced Policies' below should also be adhered to as part of our overall quality assurance framework.

7. Referenced Policies

- *Access Management Policy*
- *Assessment of Learner Policy*
- *Data Protection Policy*
- *Disciplinary Policy (Staff)*
- *Communications Policy*
- *Email and Internet Usage Policy*
- *IT Policy*
- *Learner Code of Conduct and Disciplinary Policy*
- *Records Management Policy*
- *Remote Working Policy*
- *Social Networking and Social Media Policy*

8. Monitoring and Review

This Policy will be reviewed regularly and updated as necessary if and when organisational structure or business practices and processes change. Changes in security breach patterns or new developments within vulnerabilities and threat to the College network will also result in review and update to this Policy.

All updates to this Policy and associated documents will be communicated through email to all stakeholders and a copy of all updated documentation will be posted to the staff gateway.

Appendix 1: Information Security Guidelines

Information Security Guidelines

1. Data Classification and Management

- Where data is relevant to particular parties within the College, this data should be classified by the owner and access granted in line with Records Classification Scheme. Users should reference *Records Management Policy* for data classification information.
- Access privileges to data should be granted by the data owner or manager of the area for which the data belongs to.
- Access should be granted to data in line with the *Access Management Policy*
- In the event of electronic transmission of confidential data, appropriate security precautions should be taken by the data users to ensure the data is only destined to the intended recipient who should also have relevant privileges to access data contained in the communication.

2. Network Security

All devices connected to the network of Carlow College must be covered with:

- Up to date anti-virus software;
- Up to date windows security patches;
- User authentication; and
- Active firewall (personal).

The Carlow College network is protected by an on-premise perimeter firewall which is configured through security firewall roles. All external traffic goes through this firewall and is logged and monitored for security purposes to identify an anomaly's in network traffic.

Further firewall services are in place for cloud hosted systems which are managed by IT service and are implemented by the service provider. These firewalls include:

- HEAnet
- Moodle
- Office 365
- Quercus SRMS

3. User Authentication and Access Logs

Data Users connecting to the Carlow College Local Area Network (LAN) do so through their personal logon provided by the College. Where possible, a single sign on system has been implemented for various college systems to minimise user of numerous logon credentials. All Data Users must protect and use their logon credentials in line with Carlow College *Email and Internet Usage Policy*. Data Users must not leave their workstation unattended without logging off or locking their workstation.

Network access audit logs will be kept to monitor:

- logon times and dates;
- Identity of device logged onto;
- records of failed log on attempts; and
- Data User IDs used to access devices.

System logs are monitored on all servers for troubleshooting and transaction history purposes to identify misuse of the system. Such logs include:

- Security Event logs;
- Application logs;
- Operational Audit logs; and
- Transaction and Processing logs.

As part of data security and integrity, audit trails are kept on information systems detailing user access, last logon time, file and data access and in the case of records management systems, activities carried out during the logged-on session.

4. Information Security Awareness

Data Users within Carlow College provided with relevant training and awareness to ensure appropriate safeguarding and use of data. This is carried out in line with GDPR legislation and compliance and record management.

5. Vulnerability Management

Antivirus is controlled centrally by IT Services. IT Services hold the authority to remove any device from the network for which no owner can be identified or which is believed to have the potential to compromise network security.

Each member of staff should ensure that their PC is up to date with most recent antivirus and windows update security patches. If they notice an issue with security status, this should be immediately reported to IT Services.

For all non-college devices connecting to the Carlow College network, each device must be protected with antivirus including up to date security updates. This is the responsibility of the owner of the device Windows security patches should also be configured and applied.

6. Data Availability

6.1: Software Licensing

All software licensing managed by IT will be maintained and kept up to date in line with Service Level Agreements (SLAs) and software renewal requirements to ensure continuity to access of all business applications which support college data**.** Illegal or unauthorised software must not be installed on any Carlow College device.

6.2: Data Backup and Recovery

IT Services manage backup and disaster recovery for all centrally managed data and critical systems on Carlow College network infrastructure. Incremental backups are run on a daily basis; full system backups are run weekly. Daily audit of backup jobs is carried out along with regular recovery testing.

Each department and data user is responsible for a continuity plan in their area. This involves ensuring data is included in regular system backups through the network in servers. In the event of data being stored locally, it is responsibility of the data owner to ensure that data is backed up and recoverable in the event of system non-availability.

7. Physical Device Environments and Storage

All electronic devices hosted by the Carlow College network must be stored in a suitable environment with regard to electricity, security, temperature and prevention where possible to natural disasters.

For PCs, laptops and servers which come to end of life, all data should be purged and destroyed before device is decommissioned in line with the *Records Management Policy* and *Data Protection Policy*. This falls under the responsibility of IT Services.