RCSI

RCSI DEVELOPING HEALTHCARE LEADERS WHO MAKE A DIFFERENCE WORLDWIDE

RCSI Data Encryption Policy

Document Location: http://staff.rcsi.ie/administration-and-support/information-technology/policies-and-procedures/data-encryption-in-rcsi-what-you-need-to-know

Document Control

Version	Date	Action	Author
1	25/05/2012	Create Document	Ciaran Kennedy
2	25/11/2013	Update Document	Ciaran Kennedy
3	04/01/2018	- Updated document template. - Renamed policy from "Confidential Data Policy v.2" to "RCSI Data Encryption Policy" - Added Headings: Purpose, Scope, Definitions, Policy, Roles & Responsibilities, Enforcement, and Review & Update. - Updated policy as required based on the headings above. - Communicated draft policy to JR, JL and NK for initial IT review on 04/01/2018	Ruth Meredith
4	16/04/2018	-Updated based on feedback from reviewers	Ruth Meredith
4.1	01/05/2018	-Updated wording in section 5 -Published version 4.1 as final policy	Ruth Meredith
4.2	28/04/2020	-Change in Encryption technology from Checkpoint to BitLocker updated in sections 3.1 and 3.5	Ruth Meredith

Reviewer List

Name	Title	Dept	Reviewed Date
Justin Ralph	Chief Technology Officer	I.T.	
Dónall King	Legal Counsel, Acting DPO	Legal Affairs	
Ruth Meredith	IT SDM	I.T.	
Jonathan Larkin	IT Infrastructure Manager	I.T.	

RCSI

Contents

1. Purpose 4
2. Scope 4
3. Policy 5
   - 3.1. Technology 5
   - 3.2. Data at Rest 5
   - 3.3. Portable Devices 6
   - 3.4. Data Transmission 7
   - 3.5. Encryption Key Management 8
4. Roles & Responsibilities 9
   - 4.1. Information Owner 9
   - 4.2. I.T. Department 10
   - 4.3. Line Managers 10
   - 4.4. Users 10
5. Enforcement 12
6. Review & Update 12

Appendix A 13

1. Purpose

The Royal College of Surgeons Ireland (RCSI) is legally required under the Irish Data Protection Acts and General Data Protection Regulation (GDPR) to ensure the security and confidentiality of the information it processes on behalf of its students and employees.

The RCSI is committed to the correct use and management of controls throughout the organisation. Insufficient controls or unmanaged storage, transmission or processing of information could lead to the unauthorised disclosure, theft or loss of information, fraud and possible litigation.

The purpose of this policy is to provide guidance on the use of encryption to protect information resources that contain, process, or transmit confidential and college-sensitive information. Additionally, this policy provides direction to ensure that IE and EU regulations are followed.

This policy is mandatory and by accessing any Information Technology (I.T.) resources which are owned or leased by the RCSI, users are agreeing to abide by the terms of this policy.

2. Scope

This policy represents the RCSI's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All Information Technology (I.T.) resources provided by the RCSI;
- All RCSI information systems and network resources containing information;
- All users (including RCSI staff, students, contractors, sub-contractors, agency staff and authorised third party commercial service providers) of the RCSI's I.T. resources;

The scope addresses encryption policy and controls for confidential data that is at rest (including portable devices and removable media) and data in motion (transmission security). This policy should be/is compatible with, but does not supersede or guarantee compliance with all IE and EU encryption standards

3. Policy

3.1. Technology

RCSI uses technology (BitLocker Encryption, TLS. SMTP TLS (Transport Layer Security)) for encrypting confidential and other college sensitive data. Email to and from rcsi.com email servers utilises TLS. SMTP TLS (Transport Layer Security) is the mechanism by which two email servers, when communicating, can automatically negotiate an encrypted channel between them so that the emails transmitted are secured from eavesdroppers. RCSI has configured mail flow to ensure that TLS is always used for email transmission.

3.2. Data at Rest

Note: hard drives that are not fully encrypted, e.g. have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices, may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive's unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption avoids this problem.

Confidential data at rest on computer systems owned by RCSI and located within controlled spaces and networks are protected by strict access controls that authenticate the identity of those individuals who access the specific system or data. Other compensating controls include e.g. complex passwords, physical isolation/access, network firewalls etc.

RSCI IT secures backups and stored data on SAN backup and tape in locked down server rooms in the college.

Computer hard drives or other storage media that have been encrypted shall be sanitised to prevent unauthorised exposure in accordance with the RCSI Data Destruction and Sanitisation Policy.

3.3. Portable Devices

Portable devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorised exposure of confidential data are the result of stolen or lost Portable Computing Devices. The best way to prevent these exposures is to avoid storing confidential data on these devices.

As a general practice, confidential data should not to be copied to or stored on a portable computing device or a non-RCSI owned computing device. However, in situations that require confidential data to be stored on such devices, encryption reduces the risk of unauthorised disclosure in the event that the device becomes lost or stolen.

- All users must obtain specific permission from the Information System Owner and Department Head before storing confidential data on a portable computing device or a non-RCSI owned computing device.

- Confidential information stored on portable devices including laptops, tablets, smartphones etc. must be encrypted using appropriate products and/or methods approved by IT and the DPO [such as full disk encryption with pre-boot authentication].

- Portable devices including, laptops, tablets and smartphones should not be used for the long-term storage of any confidential information.

- Portable devices including laptops, tablets and smartphones that store or transmit confidential information must have the proper protection mechanisms installed, including strong passwords, anti-virus/malware software, firewall software (where not connected to RCSI network), full disk encryption etc., and subject to needed applications being properly configured by IT.

- Removable media including CD-ROMs, DVDs, backup tapes, and USB memory drives that contain confidential information must be encrypted and stored in a secure, locked location.

- Removable media including CD-ROMs, DVDs, backup tapes, USB memory drives, etc. that contain confidential information must be transported in a secure manner. Media that is sent offsite for storage by third party must have accompanying chain of custody forms for possession tracking of media.

- Portable or removable media that contain confidential data must be in the possession of the authorised user at all times (e.g., must not be checked as luggage while in transit).

- The receiver of the removable media must be identified to ensure the person requesting the data is the one claimed.

- RCSI will inventory encrypted devices supplied by RCSI and validate implementation of encryption products at least annually.

- Data owners and users of portable computing devices and non-RCSI owned computing devices containing confidential data must acknowledge how they will ensure that data is encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. Methods to meet this requirement include:
    - Maintaining an accessible copy of the data on a server managed by RCSI IT, using procedures specified by I.T.
    - Use of whole-disk encryption technologies that provide an authorised systems administrator access to the data in the event of a forgotten key.
    - Escrowing the encryption key with a trusted party designated by the data owner and the DPO

3.4. Data Transmission

Users will follow RCSI acceptable use policies when transmitting data and must take particular care when transmitting or re-transmitting confidential data (e.g., citizen personal identification information) received from non-RCSI employees.

- Confidential information transmitted as an email message must be encrypted. Transmission of data via RCSI email is encrypted using TLS. SMTP TLS (Transport Layer Security). RCSI has configured mail flow to ensure that TLS is always used for email transmission.

- Transmitting unencrypted confidential information through the use of public web email programs, (Gmail, Microsoft mail, Yahoo etc.) is not allowed.

- Any confidential information transmitted through a public network (e.g. Internet) to and from vendors, customers, or entities doing business with RCSI must be encrypted or be transmitted through an encrypted tunnel.

- The download or installation of any Instant Messaging (IM) or online peer-to-peer (P2P) file sharing programs requires specific authorisation in writing from IT.

- Wireless (Wi-Fi) transmissions that are used to access RCSI portable computing devices or internal networks must be encrypted using WPA2 standard.

- Encryption is required when users access RCSI data remotely from a shared network, including connections from a Bluetooth device to an RCSI tablet or smartphone.

- RCSI permits the secure encrypted transfer of documents and data, up to 250MB, over the Internet using a large file transfer program via HEAnet large file sender.

3.5. Encryption Key Management

Encryption key management is managed by BitLocker Endpoint Encryption. The policy is set to 2048 bit key encryption.
This is an automated process on encryption of devices from an RCSI device.

4. Roles & Responsibilities

4.1. Information Owner

Each designated information owner is responsible for:

- The implementation of this policy and all other relevant policies within the RCSI Department or service they manage;
- The ownership, management, control and security of the information processed by their Department or service on behalf of the RCSI;
- The ownership, management, control and security of RCSI information systems used by their Department or service to process information on behalf of the RCSI;
- Maintaining a list of RCSI information systems and data that is managed and controlled by their Department or service.
- Making sure adequate procedures are implemented within their Department or service, so as to ensure all RCSI employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;
- Ensuring adequate backup procedures are in place for the information system they are responsible for;
- Conducting a regular review of the information system in accordance with this policy;
- Notifying the appropriate resources, if they suspect a user is responsible for misusing the information system or is in breach of this policy;
- Informing the appropriate resources immediately in the event of a security incident involving the system or data they are responsible for;
- Complying with instructions issued by the CTO on behalf of the RCSI.

4.2. I.T. Department

The I.T. Department is responsible for:

- The management, control, ownership, security and integrity of all RCSI network domain (LAN/WAN) on behalf of the RCSI;
- The implementation of this policy and all other relevant policies within the I.T. remit;
- Ensuring adequate procedures are in place to ensure compliance with this policy and all other relevant policies;
- Ensuring adequate technologies are in place to ensure compliance with this policy and all other relevant policies;
- Providing information owners or their nominees with audit reports and user access lists for information systems which are directly managed by the I.T. Department.

4.3. Line Managers

Each Line Manager is responsible for:

- The implementation of this policy and all other relevant RCSI policies within the business areas for which they are responsible;
- Ensuring that all members of staff who report to them are made aware of and are instructed to comply with this policy and all other relevant RCSI policies;
- Consulting with the HR, IT and Legal Department in relation to the appropriate procedures to follow when a breach of this policy has occurred.

4.4. Users

Each user is responsible for:

- Complying with the terms of this policy and all other relevant RCSI policies, procedures, regulations and applicable legislation;

- Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;

- Complying with instructions issued by designated information owners, system administrators, network administrators and/or the I.T. Department on behalf of the RCSI;

- Reporting all misuse and breaches of this policy to their Line Manager.

5. Enforcement

- The RCSI reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. This can include but not limited to suspension of network and email accounts, recovery of RCSI equipment, forensic analysis on network and/or data management activities carried out using RCSI data systems, networks and/or RCSI provided equipment RCSI staff, students, contractors, sub-contractors or agency staff that breaches this policy may be subject to disciplinary action, including suspension and dismissal as provided for in the RCSI disciplinary procedure.

- Breaches of this policy by a third party commercial service providers, may lead to the withdrawal of RCSI information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between the RCSI and the third party commercial service provider.

- The RCSI may refer any use of its I.T. resources for illegal activities to the Gardaí.

6. Review & Update

- This policy will be reviewed and updated annually or more frequently if necessary to ensure any changes to the RCSI's organisation structure and business practices are properly reflected in the policy.

Appendix A

- **Authorisation / Authorised:** Official RCSI approval and permission to perform a particular task.
- **Backup:** The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure or loss/theft etc.
- **Confidential information:** Information which is protected by Irish and/or E.U. legislation or regulations, RCSI policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact the RCSI, its students, its staff and its business partners. Some examples of confidential information include:
    - Student/ staff personal data (Except that which is restricted)
    - Patient /client medical records (Except that which is restricted)
    - Unpublished medical research
    - Staff personal records
    - Financial data / budgetary Reports
    - Service plans / service performance monitoring reports
    - Draft reports
    - Audit reports
    - Purchasing information
    - Vendor contracts / Commercially sensitive data
    - Data covered by Non-Disclosure Agreements
    - Passwords / cryptographic private keys
    - Data collected as part of criminal/HR investigations
    - Incident Reports

- **RCSI Network:** The data communication system that interconnects different RCSI Local Area Networks (LAN) and Wide Area Networks (WAN).
- **Information:** Any data in an electronic format that is capable of being processed or has already been processed.
- **Information Owner:** The individual responsible for the management of a RCSI Department/School/Faculty.
- **Information Technology (I.T.) resources:** Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the RCSI.
- **Information System:** A computerised system or software application used to access, record, store, gather and process information.
- **Line manager:** The individual a user reports directly to.

- **Network Administrators:** These are the individuals responsible for the day to day management of a RCSI network domain. Also includes RCSI personnel who have been authorised to create and manage user accounts and passwords on a RCSI network domain.
- **Network Domain**: A set of connected network resources (Servers, Computers, Printers, Applications) that can be accessed and administered as group with a common set of rules
- **Personal Information:** Information relating to a living individual (i.e. RCSI employee, student) who is or can be identified either from the Information or from the information in conjunction with other information. For example: - an individual's name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.
- **Privacy:** The right of individual or group to exclude themselves or information about themselves from being made public.
- **Process / Processed / Processing:** Performing any manual or automated operation or set of operations on information including:
    - Obtaining, recording or keeping the information;
    - Collecting, organising, storing, altering or adapting the information;
    - Retrieving, consulting or using the information;
    - Disclosing the information or data by transmitting, disseminating or otherwise making it available;
    - Aligning, combining, blocking, erasing or destroying the information.
- **Remote Access:** Any connection to the RCSI network(s) or information systems that originates from a computer or device located outside of the RCSI network.
- **Restricted Information:** Highly sensitive confidential information. The unauthorised or accidental disclosure of this information would seriously and adversely impact the RCSI, its students, its staff and its business partners. Some examples of restricted information include:
    - Unpublished financial reports
    - Strategic corporate plans
    - Sensitive medical research
- **System Administrator:** The individual(s) charged by the designated system owner with the day to day management of RCSI information systems. Also includes the RCSI personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.
- **Third Party Commercial Service Provider:** Any individual or commercial company that have been contracted by the RCSI to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the RCSI.
- **Users:** Any authorised individual using any of the RCSI's I.T. resources.