Encryption Policy

ROWAN UNIVERSITY POLICY

Title: *Encryption Policy*
Subject: *Information Security*
Policy No: *ISO:2016:05*
Applies: *University-Wide*
Issuing Authority: Senior *Vice President for Information Resources and Chief Information Officer*
Responsible Officer: *Director of Information Security*
Date Adopted: *04/01/2016*
Last Revision: *01/31/2024*
Last Review: *07/03/2018*

I. PURPOSE

The purpose of this policy is to provide Rowan University communities guidance on the use of encryption to protect Rowan University's information resources that contain, process, or transmit confidential and or sensitive information.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the University's Director of Information Security shall implement and ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy.

III. APPLICABILITY

This policy applies to all employees, faculty and staff; student workers including interns whose job function falls within scope of this policy by virtue of the types of data access which they are granted, either explicitly or implicitly (such as access to network shares or documents containing data covered by the scope of this policy); and, all contractors, vendors and any other 3rd parties entrusted with University Highly Sensitive, or Sensitive Data.

IV. DEFINITIONS

1. *Confidential Information* – Is a set of rules or a promise that limits access or places restrictions on certain types of information
2. *Cryptographic algorithms***-** Is a mathematical algorithm, used in conjunction with a secret key, that transforms original input into a form that is unintelligible without special knowledge of the secret information and the algorithm**.**
3. *Cryptographic keys***-** Is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.
4. *Encryption* – A process by which data is transformed into a format that renders it unreadable without access to the encryption key and knowledge of the process used.
5. *Encryption Key* – A password, file or piece of hardware that is required to encrypt or decrypt information, essentially locking and unlocking the data.
6. *Sensitive Information***-** Any information that can be used to identify you or another person is sensitive information.

V. REFERENCES

1. The Rowan Information Security Policyhttp://www.Rowan.edu/InfoSecurity/

VI. POLICY

1. It is the policy of Rowan University to employ encryption to mitigate the risk of disclosure or alteration of confidential and or sensitive information within Rowan University's information systems infrastructure or through outsource services example "Cloud Storage Services and or Software as a Service".
2. Requirements:
    a. All laptop computing devices owned by Rowan must employ whole disk encryption, as defined in this policy, to protect University data regardless to how sensitive this data is.
    b. All Rowan University owned and BYOD desktop computing devices containing Rowan's confidential and/or sensitive data must employ whole disk encryption, as defined in this policy, to protect this data.
    c. All Rowan University owned and BYOD Mobile devices such as Personal Digital Assistant (PDA), Tablets and Smartphones containing Rowan confidential and/or sensitive data must employ encryption, as defined in this policy, to protect this data.
    d. Databases, network shared systems which would include but be limited: (Container, Volume, Files, Folders, etc.)
        i. Sensitive data not housed in a University approved datacenter must be encrypted.
        ii. Data in motion: End user facing connections over which confidential or sensitive data may be exchanged should be encrypted in transit when leaving a datacenter in order to prevent unintended exposure of data where technically practicable.
    e. All portable media containing Rowan University confidential and/or sensitive data must employ encryption, as defined in this policy, to protect this data.
    f. All data contained within email classified as confidential or sensitive leaving Rowan University's managed datacenters must employ encryption in transit where technically practicable, as defined in this policy, to protect this data in transit.
    g. Portable computing devices and desktop computing devices that contain Rowan confidential or restricted data solely in transient data files (i.e. files that do not remain on the computing device after a system power down or reboot) are not required to employ whole disk encryption to protect the data, but it is highly recommended to do so when feasible.
    h. Encryption implementation standard
        i. Only encryption solutions approved by the Offices of the Chief Information Officer and Director of Information Security may be utilized to satisfy the requirements of this policy.
        ii. The whole disk encryption solution will centrally manage whole disk encryption client software for all systems, including encryption format, key management, and logging.
        iii. Based on the classification level assigned to a data asset, data at rest shall be encrypted in accordance with the university Data Classification Policy when the data does not reside in a Rowan University managed and physically secured data center.
        iv. Based on the classification level assigned to a data asset, data in transit, external to Rowan University managed data centers, shall be encrypted in accordance with the university Data Classification Policy.
        v. The exporting or international use of encryption systems shall be in compliance with all United States federal laws (especially the US Department of Commerce's Bureau of Industry and Security's Export Administration Regulations) or appropriate international laws.
        vi. Technology owner will maintain documented procedures for supported cryptographic algorithms, by data classification level, based on documented baselines provided and maintained by the ISO. Technology owner procedures may include accommodations for each technology agreed upon between technology owner and ISO.
        vii. The Technology Owner, in accordance with ISO standards, will maintain documented procedures for cryptographic key management which include documentation on the processes of:
            - Generating cryptographic keys
            - Distributing cryptographic keys
            - Escrowing cryptographic keys
            - Enabling authorized users to access stored cryptographic keys

- Changing and updating cryptographic keys
- Revoking cryptographic keys
- Archiving cryptographic keys
- Auditing and logging cryptographic key management

viii. Rowan University retains the right to decrypt data using the centrally maintained key(s) to support operational requirements or when approved by the ISO, CIO or general counsel.

i. Deployment responsibilities
   i. It is the responsibility of the Data Owner and Technology Owner to ensure that systems requiring encryption are identified, and that encryption is properly deployed on these systems
j. End user responsibilities
   i. Users must report any known, unencrypted restricted data on portable computing devices to IRT support staff and request assistance in removing the data or acquiring encryption software.
   ii. Users must not attempt to disable, remove, or otherwise tamper with the encryption software

3. Special Circumstances for RowanSOM
   a. Due to the highly confidential and/or sensitive nature of data used at the Rowan University School of Osteopathic Medicine (RowanSom), all devices, including but not limited to those referenced above in sections E through F, must employ whole disk and USB encryption.
   b. EXCEPTIONS TO SPECIAL CIRCUMSTANCES
      i. Any RowanSOM device which has the sole purpose of serving multiple users (not assigned to an individual, i.e Classroom/Lab devices) is explicitly exempt from having USB encryption enabled, provided the machine is not used to read, store, or access confidential and/or sensitive data.
      ii. Documentation of these devices must be communicated to the Information Security Office (ISO) in writing at the time the device is placed into service or before the USB encryption has been disabled. The ISO will maintain a master list of all devices for which USB encryption has been disabled.
      iii. Any exception that does not meet the above requirements must be approved by the ISO. All requests must be made using the Rowan Policy Exception form and be submitted to the ISO for approval by the Director of Information Security.
4. NON-COMPLIANCE AND SANCTIONS
   a. Violation of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school, and may subject the violator to penalties stipulated in applicable state and federal statutes.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer