Encryption (Cryptographic Protection) Policy

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations, and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective
The policy and associated guidance provide the practices WashU will utilize to protect the integrity and confidentiality of information stored, transmitted, transferred to portable media, and sent through messaging systems to entities external to the university.

Applicability
This policy is applicable to any WashU network, infrastructure, system, device – WashU owned or personal, and application that create, store, or transmit protected information.

Audience
The audience for this policy is all WashU faculty, staff, and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

Policy
Encryption is used to secure information by making it unreadable to unauthorized individuals. WashU requires encryption of protected information contained on all electronic devices, mobile media, laptops, workstations, servers, and external hosted sites that are not located in Approved Secure Data Centers. The Approved Secure Data Centers are defined as data centers that have had a formal risk assessment on the physical and logical controls completed by the Office of Information Security (OIS) and the Internal Audit Office with no findings that would render the data center unsecured.
WashU Community members are responsible for the physical security of any devices containing confidential and/or protected information and must report any device that is lost or stolen as soon as it is possible.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Data Classification</th>
<th>Encryption Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled Unclassified Information (CUI)</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>FISMA</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>ePHI/Clinical Data</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>Nuclear Regulatory Information (NRC)</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>Chemical Facility Anti-Terrorism Standards</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>PCI</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>Personal Identifiable Information (PII)</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>General Data Protection Regulation (GDRP)</td>
<td>Protected</td>
<td>Recommended</td>
</tr>
<tr>
<td>FERPA (PII)</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>FDA Part 11</td>
<td>Protected</td>
<td>Yes</td>
</tr>
<tr>
<td>dbGaP</td>
<td>Confidential</td>
<td>Recommended</td>
</tr>
<tr>
<td>Financial Information</td>
<td>Confidential</td>
<td>Recommended</td>
</tr>
<tr>
<td>Legal Documents</td>
<td>Confidential</td>
<td>Recommended</td>
</tr>
<tr>
<td>Human Resources (HR)</td>
<td>Confidential</td>
<td>Recommended</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>Confidential</td>
<td>Recommended</td>
</tr>
<tr>
<td>De-Identified Research Data</td>
<td>Confidential</td>
<td>Recommended</td>
</tr>
<tr>
<td>Academic Content</td>
<td>Public</td>
<td>No</td>
</tr>
</tbody>
</table>

**Storage (Encryption at Rest)**

All electronic devices which receive, store, and/or transmit protected information and are not located in an Approved Secure Data Centers must use WashU-approved encryption methods that comply with applicable laws and regulations to secure the information stored or transmitted outside the secure clinical network.

- Servers that are not located in an Approved Secure Data Center are required to have all information stores of protected information encrypted.
- Servers in Approved Data Centers that contain information of various classes and are accessed via public networks shall have protected information encrypted.
- Protected information contained on laptops or workstations are required to be encrypted - file, folder, or full disk.
- Files will be encrypted prior to storage on devices that are not able to be encrypted.
- Any and all mobile devices (e.g. smart phones and tablets) that connect to the secure clinical network that may contain or transmit protected information (e.g. email) are required to accept information security standards to encrypt and protect the devices.
- External storage media (e.g. backup tapes, removable drives, etc.) are required to have protected information encrypted.
- Encryption will not be removed or disabled from any device without the approval of the CISO.

Existing systems and applications containing protected information which cannot use encryption because of technology limitation, but have compensating controls, may be granted a special exception by the OIS. However, these systems and applications will be required to have a formal risk assessment performed by the OIS to ensure that major risks are addressed via compensating controls to protect the data in lieu of encryption. Exceptions will be reviewed periodically and removed when a suitable solution is available.

Transmission (Encryption in Transit)

In order to ensure the confidentiality and integrity of protected information WashU will implement technical security measures to guard against unauthorized exposure of protected information during transmission on internal network or to an external location.

- Files that contain protected information that are transmitted across the Internet (e.g. email attachments sent to non-WashU or BJC addresses, or file transfers to other entities) will need to have the attachments encrypted or use a WashU secure encrypted method to deliver that information.
- Internal transmissions between WashU and BJC are considered secure.
- All transmissions of protected information across public infrastructures including, but not limited to, personal email accounts, public cloud services, vendor systems, must either encrypt the information or encrypt the connection between the sending and the receiving entity.
- All transmissions of protected information across public networks must also ensure the integrity of protected information that it is not improperly modified without detection while in transit.
- WashU community members are responsible for ensuring an approved method is used to transmit WashU information that has been classified as requiring encryption.
WashU Community is responsible for the transmission of protected information will follow the Transmission Security Standard and Encryption Standard to ensure a secure mechanism will be used to transmit the information. If not able to meet the requirements, an exception may be requested from the OIS.

**Key Management**
Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting processes and procedures.

IT will document the key management:
- Generation
- Distribution
- Storage

**Certificates**
Certificates deployed on WashU systems will be centrally distributed. They will be obtained by a trusted Certificate Authority.

**Policy Compliance**
The OIS will measure the compliance to this policy through various methods, including, but not limited to - reports, internal\external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the OIS in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources, or the Office of Student Conduct.

**Related Policies**
Mobile Device Security Policy
Incident Reporting Policy
Information Classification Policy

**Reference**
Secure Storage and Communications
NIST publication FIPS 140-2
NIST Policy on Hash Functions
WU Controls workbook; Control SC 8, 12, 13, 17, 28
Encryption Standard

**Policy Review**
This policy will be reviewed at a minimum every three years.

**Title:** Encryption Policy  
**Version Number:** 2.0  
**Reference Number:** SC-01.01