JOHNS HOPKINS

Institutional Computing Standards

Standards and Guidance for Encryption

Approved by the ICSC in May 2007, Revisions approved in March 2012, March 2016 and February 2020

I. Table of Contents

III. Introduction

A. Background

One of the most important tools for securing data is encryption. For data in transit across public networks such as the Internet, encryption is one of the few means available to maintain security. Strong encryption protects confidentiality in route and, if the underlying system is configured properly, helps authenticate recipients of the transmission. For data at rest, encryption provides an additional layer of protection and is becoming increasingly important for regulatory compliance. The quality and usability of encryption tools has improved dramatically over the last few years, and it is now possible to deploy strong standards-based encryption for a number of purposes.

B. Policy

Johns Hopkins Information Technology Policies address encryption in a number of settings. Policy will be addressed in each section below.

C. Audience

The target audience for this document include power users and administrators of Johns Hopkins IT Resources. Users may benefit from this standard also but they should work with their professional IT staff regarding complex deployments of encryption.

D. Scope

This document serves as both a set of standards and checklist encryption.

E. Enforcement

Failure to follow these standards may be considered a violation of *Johns Hopkins Information Technology Policies,* which are incorporated by reference. For systems that store, process, or transmit E-PHI, failure to follow these standards may be a violation of *Johns Hopkins HIPAA Privacy and Security* policies, which are incorporated by reference.

IV. Encryption Standards

Johns Hopkins requires the use of standards-based encryption deployed according to good practice. Encryption used for applications, storage and transmission of information at Hopkins must follow NIST guidance for standard types of encryption including AES, RSA, Diffie-Hellman and elliptic curve. Encryption for critical assets and Restricted information must follow NIST-published standards. Any encryption protocol or process that is not approved by NIST must be approved by the Hopkins Chief Information Security Officer. It is the responsibility of owners, developers and administrators to ensure that systems do not fall out of compliance with NIST standards or those included herein.

In general, what the Johns Hopkins IT Policies term “Restricted” information must be encrypted for transmissions across public networks or when stored on mobile devices or media. Users should avoid clear text transmission of any Restricted information even within the JH Network. In particular, voluminous or otherwise high risk datasets should always be encrypted when sent.

Restricted information should always be encrypted when stored on mobile devices and media, such as laptops, handheld, back-up tapes, etc. It may also be advisable to encrypt other Restricted information at rest, although most current database technologies impose some loss of performance when encrypting data tables.

V. Information Technology Policies

A. Policy

(c) SECURITY RESPONSIBILITIES FOR CUSTODIANS OF RESTRICTED INFORMATION

2. Transmission – It is prohibited to transmit Restricted information across public networks (i.e. the Internet) unless encrypted. Transmission of this type often involves insecure delivery. Examples include but are not limited to:

   a. Emails to non-JH addresses including, for example, gmail, nih.gov, harvard.edu, etc.

   b. Automatic mail forwarding to external systems

   c. Instant messaging across non-JH messaging platforms, including AOL, Trillian, etc.

   d. Unencrypted pagers

JH has tools for encrypting transmissions, including secure email, instant messaging and file sharing. Password protection of Microsoft Office attachments is also a sensible protection for transmission of Restricted information to external entities.

3. Mobile Encryption -- All laptops and mobile devices, including personally owned devices, must have full disk encryption installed and activated prior to the receipt or storage of Restricted information. Laptop computers and mobile devices at Johns Hopkins Medicine must be encrypted as a matter of course. As a matter of prudence, any device reasonably likely to be used to store Restricted information should have such encryption activated.
4. Portable Storage Media Encryption – all portable storage media that store Restricted information (e.g. backup tapes, flash drives, DVD's) must be encrypted at the file, folder or device layer to ensure that all Restricted information is protected.
5. Desktop Encryption – storage of Restricted information on desktop computers poses risk of loss or theft. Therefore, desktop computers must have full disk encryption installed and activated prior to the receipt or storage of Restricted information. Desktop encryption is a relatively new requirement, and implementation among divisions and entities may take place in phases. Implementation of desktop encryption at Johns Hopkins Medicine is deemed as high priority.
6. Server Encryption -- All servers storing Restricted information (e.g. file servers, email servers, databases) must be stored in a JH-managed or approved data center or otherwise secure area (see Data Center Security Standards and Guidance, http://www.it.johnshopkins.edu/policies/standards.html). Server encryption is advisable for servers in general, and encryption of data-at-rest is required for any server storing Restricted information not located in a data center compliant with ICSC Data Center Security Standards.

B. Encrypted Authentication

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. While the JH Network has security controls, it is still poses some risks. Therefore, credentials should be encrypted even if transmissions never leave the JH Network. Even in cases, where payloads are clear text, authentication must be encrypted.

In particular, services that pass credentials insecurely such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

In addition, passwords and other authentication credentials may not be stored on any system without both applying standards based encryption and appropriate slating algorithms. Simply hashing passwords is unacceptable.

VI. Certificate Services and Configuration

A. Certificate Services offered through IT@JH

Hopkins maintains a Public Key Infrastructure (PKI) from which to support internal communications and applications. It uses third party management tools and includes features such as automatic generation and renewal of keys. The PKI follows all applicable NIST standards and generates keys of 2048 bit RSA in order to maintain security through the next five years. It is strongly encouraged that developers or administrators that require certificates for applications to be used exclusively in the Hopkins environment, use our Hopkins PKI and contact IT@JH for support. Hopkins maintains a compliant “chain of trust” on its certificates, and it is important that administrators maintain it downstream.

As of 2020, Hopkins also has an enterprise agreement with Comodo for certificates, and these are widely used throughout the environment. We encourage use of enterprise-endorsed (such as Comodo) certificates for systems that communicate outside the Hopkins environment. These have also been upgraded to 2048 bit RSA.

Self-signed certificates are strongly discouraged except for use in small scale applications, with limited users and no external visibility. All certificates used in our environment should have a key length of 2048-bit RSA or 256-bit ECDSA (elliptic curve).

It is also important to ensure that certificate hostname coverage (e.g. for both www.something.jhu.edu and something.jhu.edu) is sufficient and to ensure expiration dates are well understood especially where there are two or more certificates in the chain of trust. One approach to addressing this problem, wildcard certificate names, are discouraged. Wildcard certs can pollute the certificate namespace. Certificate expiration surprises are a common problem and preventing them requires careful planning, especially when there are development, testing and production hosts deployed.

B. Certificate management standards

It is strongly encouraged that systems use the current certificate infrastructure at Hopkins for issuance and management of keys. If circumstances require use of other certificates or Certification Authorities (CA), the following standards should be considered a baseline. Prior to implementation, careful attention should be paid to situation-specific requirements of the certificate/key infrastructure.

As an educational institution, Hopkins rely on the inCommon federation as our preferred CA. Use of another CA requires written authorization from the Hopkins Chief Information Security Officer. CA’s are evaluated on a number of criteria including market share, security practices and reputation, NIST compliance, services offered (e.g. Certificate Revocation Lists) and support models.

C. Protection of Private Keys

It is critically important that server administrators understand basic key management. In 2014, Heartbleed and other vulnerabilities demonstrated the importance of effective key revocation and generation in a relatively short time frame. Keys should be generated on trusted computers, password-protected, regenerated with new certificates after potential compromise, reviewed biennially and renewed periodically.

D. Secure Protocols

One of the most common, and yet most easily remedied, failures involve allowing insecure protocols, cipher suites and key lengths. Many medical applications use old server technology and deem it acceptable for users to interact through deprecated browsers, that these problems are common in our sector.

A Tenable/NESSUS scan will indicate deprecated protocols. In addition, for externally facing web servers, one can easily run an on-line test (with letter grades from SSL Labs at Qualys) (https://www.ssllabs.com/ssltest/) or through nmap (nmap -p T:<PORT> --script ssl-enum-ciphers <SERVERNAME>).

As of July 1, 2019, current best practices include:

- Protocol security for SSL/TLS is as follows:
  - SSL v.2 and v.3 are prohibited is vulnerable to POODLE attacks and should be avoided
  - TLS v.1.0 and v.1.1 are prohibited in part due the POODLE attack can downgrade negotiation to SSL 3.0
  - TLS v 1.2 and 1.3 are acceptable.

- Other protocols
  - SHA-1 and MD5 may be only used for integrity checks and not communications security
  - SHA-2 (which is a superset of several hash functions) and the current preferred deployment,SHA-256, are acceptable (SHA-3 functions – released by NIST in August 2015 – should also be acceptable)

Websites and services should avoid mixed mode (e.g. partially HTTP and HTTPS) operation to avoid lateral attacks.

E. Secure Cipher Suites

Deploying secure cipher suites can be more complex than using protocols:

- Preference for 256-bit -- No cipher suites should be allowed with bit lengths less than 128, we require that 256-bit be accepted as an earlier option than 128
- NULL cipher suites are prohibited as fallback in protocol negotiations
- 3DES is allowed but not for web communications as its key length and performance are sub-optimal
- RC4 is prohibited and should be disabled
- Disable TLS compression, due to CRIME attacks that can open up attacks against session cookies
- Disable client-initiated renegotiation; server initiated renegotiation should be evaluated because of occasional vulnerabilities

VII. Website encryption

All new or websites undergoing that either are themselves enterprise websites or connect operationally (i.e. not simply an html link) to an enterprise Hopkins website must conduct all transactions over https/TLS (e.g. port 443). Any port 80 http transaction must be redirected to it encrypted counterpart. In addition, site owners and administrators should ensure that all deprecated protocols and ciphers are disabled consistent with Hopkins standards.

For these purposes, connections to enterprise sites include authentication through JHED or information passing to a Hopkins enterprise site (e.g. jhu.edu, hopkinsmedicine.org). There are substantial risks in mixed mode web traffic that can be alleviated by fording all web traffic through https.

Even sites without direct enterprise connections are encouraged to adopt https, and administrators and technical staff are required to develop plans for migrating over existing sites.

VIII. Secure Transmission with Secure File Transfer Protocol (SFTP) for Large Files

IT@JH has an enterprise SFTP tool for large and/or file transfers called MOVE-IT. This tool deploys a number of methods – SFTP, FTPS, https, for both puts and gets – to securely transfer files. Other tools may be used so long as they meet security and encryption standards set forth in this document.

IX. Secure Transmissions of Restricted Systems

Enterprise applications that send Restricted information as part of ordinary operations (i.e. nearly every clinical system) must encrypt those communications between systems , including client/server communications. Exceptions to this general policy may be grated for performance sensitive interfaces where both ends of the connection are on the same network segment inside a Hopkins enterprise data center.

X. Secure Transmissions – E-mail

Johns Hopkins requires encryption for transmissions of Restricted information outside the Hopkins network. OneDrive is an appropriate tools for this type of sharing. This protects the initial transmission and prevents secondary transmissions by recipients forwarding messages.

For more routine email communications to recipients outside of Johns Hopkins, senders intending to send PHI (this service is principally geared toward Johns Hopkins Medicine) can encrypt messages using our Cisco/Ironport email gateway product. Users should include the following text -- [secure]. The message will then be encrypted at the email gateway which is the last stop before sending to the Internet. The recipient will then register to a Cisco portal site (unconnected to Johns Hopkins authentication) in order to receive that message and subsequent message sent through this service. This service is being deployed by department in the Exchange environment for Johns Hopkins Medicine. For more information, see http://www.it.johnshopkins.edu/services/email/.

For organizations for which Hopkins routinely communicate via email, it is advisable to consider establishing a dedicated TLS connection between the Hopkins email gateway and that of the other organization. Such connections will encrypt all communications through between the two parties using these gateways. Before asking the Johns Hopkins messaging team to establish such a connection, you must contact IT staff at the interlocutor organization to ensure that it can establish such a link on its end.

XI. Text Messaging

Users should refrain from sending Restricted information through standard text messaging. The wire security of such text messages, while stronger perhaps than TCP/IP, may not be adequate for such information. In addition, there is always the possibility of the text being sent to the wrong individual.

As of 2020, Johns Hopkins provides a CORUS testing service that uses web services to encrypt text messages between Hopkins users and provides better support for ensuring that text messages are sent to the correct recipient. Corus requires a smart phone client and user registration. In addition, Epic texting is considered appropriate end to end encryption.

XII. Credit Card Transactions

All Hopkins enterprise involving Hopkins merchant services (i.e. payment transactions) credit card transactions involving credit card numbers and/or CV2 codes must utilize an external payment gateway. Such transactions originating on Hopkins-owned or managed equipment must have PCI certified end-to-end encryption (e.g. encrypted key pads).

XIII. Data at Rest

Encryption of Restricted information at rest is required for Restricted information outside a Johns Hopkins enterprise data center. Inside a data center, systems owners and administrators are required to conduct a risk assessment regarding technical capabilities, performance and feasibility of encryption of data at rest. Typically, this requires server-level encryption to protect against physical theft and virtual machine encryption where possible.

Restricted information stored in cloud services must use encryption at-rest where possible. Key management of cloud services is an emerging concern and should be considered in light of the Hopkins cloud Security standards.

XIV. Device Encryption Table (2020)

Encryption Tools	Method/Approach	Useful For	Not Useful For	Hints
MS Office Encryption (Versions 2007+)	Password protection of Office documents uses encryption by default.	Saving one file in several places, emailing a file	Multiple files, Where access logs are required.	This can be slow to encrypt >10GB
Windows Bitlocker – Windows 8.x, 10 (Pro or Enterprise)	Only supported tool for full disc encryption of Windows workstations. In the JH corporate image with professional key management and recovery services through the MBAM utility.	Full disc encryption – this is the preferred Windows solution because it is included in our desktop management suite	Laptops without TPM chips have a clunky a token based key management system. Devices with home-use Windows must be upgraded to enterprise level.	Bitlocker is an enterprise solution primarily and directed toward enterprise versions of Windows.
Apple FileVault2	Apple OS X full disc encryption for versions > 10.7	Free full disc encryption	Works in nearly every use case.	JHM may require management agent to ensure that JH Network recognizes the encrypted device.
7-zip	http://www.7-zip.org Freeware	Encrypts all types of files in folders. Useful for saving on storage devices, e-mail, etc. All major platforms.		Works well with other products. Make sure to select encryption and interoperability is better if you save as .zip format.
Dell Data Protection	Disc encryption for volumes (other than boot sector) that is cross-platform and does not require a TPM chip be installed.	Useful for departments that have machines without TPM.	Management agent to prove encryption for JHM network must be installed separately.	Other tools such as PGP, Sophos and McAfee can be used for this.
DiskCryptor	www.diskcryptor.net This free tool replaces full disc encryption tool TrueCrypt for full disc encryption. It is not supported by the enterprise, and requires some technical sophistication to manage keys.	Full disc encryption for Windows. Works well with desktops. Easy to install.	May cause issues with laptop sleeping.	Other tools such as PGP, Sophos and McAfee can be used by individuals for this purpose. All such solutions require local key management.
Veracrypt	Folder based encryption as an alternative to 7-zip. It is a fork of deprecated TrueCrypt and should be used in place of Truecyrpt.	Supports all major platforms. Similar to TrueCrypt in usability. Excellent for saving large files or folders.	Inexperienced users may struggle with mounting directories	Other tools include Bitlocker-to-Go.
Encrypted removable storage – Kingston Data Traveler, IronKey	Can be purchased on Amazon and other on-line retailers. IT@JH maintains several hundred for distribution as needed.	All major platforms	Host security tools may interfere with use.	
iOS Encryption	iPhones in versions of 3GS and later, all iPads include hardware encryption for data at rest. Once a PIN is required, it is activated automatically.	On by default, cannot be turned off by user.		User must have a pin for it to be effective.
Android Encryption	Versions of Android 2.3.3 and later support strong encryption. Nearly all Android devices from major manufacturers now support encryption, and most turn on by default.	Activation is relatively simple to activate but varies by manufacturers		Check encryption state by model number
Microsoft Surface	Surface RT is encrypted by default. Surface Pro requires user activations of Bitlocker.	Follows standard Windows 10 protocols		

XV. References

None.

XVI. Appendices

None.