

IT Security Standard:

Encryption Tools and Protocols

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: *Information Technology (IT) Security* regarding encryption of data. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines procedures for use of cryptographic tools, protocols and algorithms at Bellevue College.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat and Vulnerability Analysis

Cryptography and encryption are used as security tools at Bellevue College in an attempt to address two fundamental issues: confidence in the security of data and authenticity of data that has been manipulated. The specific software tools used do not present any threat or risks. As such, this standard does not so much address risk as it improves the likelihood that high quality algorithms and tools will be used when cryptographic methods need to be employed to protect confidential and sensitive data.

Standard

1. General

- a. Encryption used at Bellevue College to protect data identified as “Sensitive”, “Confidential”, or as “Information Requiring Special Handling” within the Bellevue College IT security standard addressing “*Data and Information Security*” will meet the expectations of this standard.
- b. Digital signing of legal/contractual documents for and with the State of Washington is in some cases controlled by provisions of RCW 19.34 and WAC 434.180.
 - i. The uses of encryption considered here are for a more basic authentication of communications and other areas, not considered within the scope of those laws at this time.
 - ii. If Bellevue College develops a program regarding digital signing of legal or contractual documents, the procedures and tools/application chosen for use will fully

meet the expectations identified within those state laws and will reflect the current best security practices at the time of implementation.

- c. All algorithm routines used in Bellevue College applications will be a generally-accepted algorithm available within the technology community. Within the context of this standard, “generally-accepted” is defined as an open and published algorithm that has received extensive peer-review and has no currently known weaknesses or exploits.
- d. Bellevue College staff will not attempt to create or implement “homegrown” algorithms for either data encryption or for message digest hashing.
- e. Aside from those specific algorithms identified below, other generally-accepted algorithms can be submitted to the Bellevue College IT Security Administrator and/or Dean of Information Resources, or designees, for review and possible inclusion in the approved list of algorithms.

2. Data Encryption Algorithms

- a. Currently, Bellevue College recognizes the following symmetric-key (or secret-key) algorithms as meeting this criteria:
 - i. Rijndael—also known as the Advance Encryption Standard (AES)—is the preferred algorithm.
 - ii. Twofish, Blowfish, RC4, IDEA, CAST-256 are generally considered strong algorithms, and may be used if a specific situation warrants it and Rijndael is inappropriate for the task.
- b. Currently, Bellevue College recognizes the following asymmetric-key (or public-key) algorithms as meeting this criteria:
 - i. RSA, using no less than 1024 bit keys, and DSA, using no less than 1024 bit keys, are the preferred algorithms.
 - ii. Diffie-Hellman may also be used, if a specific situation warrants.

3. Message Digest (Hash) Algorithms

- a. Currently Bellevue College recognizes the following digest algorithms as meeting this criteria:
 - i. SHA-1, SHA-256, SHA-284, and SHA-512 are all NSIT standards, and are the preferred algorithms.

4. Key Management

- a. Management of encryption keys, which are often the same as passwords, can be challenging. Protections outlined within the Bellevue College IT security standard addressing “*Password Management*” will apply.

5. Specifically approved Tools and Protocols

There are several common cryptographic applications that are, when used correctly, considered by the security community to be safe and of high quality. These tools will be used by Bellevue College without further review. In all cases, key lengths will be specified to meet current cryptographic standards.

- a. Pretty Good Privacy (PGP) and its functional work-a-likes--OpenPGP and Gnu Privacy Guard (GPG).
 - i. These can be used for public or secret key encryption, as well as signing. Since PGP generally is used in a public key mode, key lengths will be at least 1024 bits.
- b. Secure Socket Layer (SSL) is the standard for securing HTTP communications, though it can be used to secure other protocols, as well.
 - i. Key lengths of 128-bit are considered acceptable for financial and personal data; key lengths less than that are not considered safe.

- c. Secure Shell (SSH) is the standard for a secure replacement to telnet-like terminal access and ftp-like file copying.
 - i. SSH also has the ability to establish secure channels through which other TCP/IP protocols can be tunneled, like an ad-hoc VPN.
 - ii. Key lengths will be at least 1024 bits, and the SSH v.1 protocol will be disabled.
 - iii. More information on the use of SSH at Bellevue College can be found in the Bellevue College IT security standard addressing "[*SSH Configuration*](#)."
- d. The Secure Internet Protocol (IPSec) is the standard set by the Internet Engineering Task Force (IETF) for encrypting and authenticating communications between two networked devices at the Internet Protocol (IP) layer of the network stack.

6. Cautions

There are many other software tools in common use that advertise "encryption" capabilities.

- a. Many of these tools do a very poor job with respect to implementing appropriate encryption. While these products may be leaders in their various areas of specialization, they do not meet the expectations regarding strong cryptography.
- b. Because of this, the so-called encrypted files associated with these applications can be broken in a short amount of time on ordinary workstation class computers.
- c. Common examples of these applications include Microsoft Office products and WinZip's file compression tool.
- d. If a file needs to be protected by cryptographic means, PGP or an equivalent product will be used.

7. Secure Data Storage

Currently no Bellevue College protected data is required to be routinely stored in an encrypted state. Protected Bellevue College data are secured requiring login credentials to be used to access secure computing resources. However, if the need to store data securely using encryption becomes necessary, either for routine use or archival purposes, written procedures for such secure data storage will be developed and approved by the Dean of Information Resources or authorized designee. At a minimum, any procedures developed must:

- a. Ensure that authorized IT support personnel have the ability, if necessary, to decrypt stored data through a documented and authorized process.
- b. Ensure that necessary decryption can take place at any time during an adequate recovery period identified within the written process.
- c. Protection of information regarding the encryption and decryption methods takes place in accordance with applicable Bellevue College IT security standards.
- d. Ensure that the encryption methods and processes do not allow the data to be understood by any unauthorized entity gaining access to it.
- e. Ensure that alteration of the intended content can be detected by support personnel.

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to Bellevue College IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Associate Dean of Student Success (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

1. SBCTC-IT IT Security Standard—*Encryption*, March 10, 2003.
2. Bellevue College Policy #5250: *Information Technology (IT) Security*
3. Bellevue College IT Security Standard: *Data and Information Security*
4. Bellevue College IT Security Standard: *SSH Configuration*
5. RSA Laboratories, *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1*, 2000, RSA Security Inc., http://www.rsasecurity.com/rsalabs/faq/files/rsalabs_faq41.pdf
6. Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code*, 1993, John Wiley & Sons, Inc,
7. Counterpane Labs, *Counterpane Labs Publications*, 2006, Counterpane Internet Security, Inc. <http://www.counterpane.com>
8. *SANS Info Sec Reading Room: Encryption and VPNs*, 2006, SANS, <http://www.sans.org/rr/whitepapers/vpns/>

Effective Date: July 2003
Date Last Modified: April 12, 2009