



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-05-03-2009

DIVISION OF INFORMATION TECHNOLOGY

Data Encryption Policy

Date of Last Revision 06/09/2009

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Purpose

- a. Information held by public organizations can include social security numbers, credit cards numbers, and home addresses of Rhode Island citizens. Government, in particular, is responsible for information that protects public health and public safety. Individuals with malicious intent can easily acquire information being transmitted electronically unless appropriate security measures are applied, such as encryption.
- b. If detected, the credentials employees use to access data and systems can provide unauthorized access which can lead to critical data being modified, deleted and ultimately unavailable. For these reasons very sensitive information must be protected through encryption methods.

2. Scope

- a. This policy applies to all state agencies that fall under the Executive Branch of Rhode Island state government.

3. History

- a. This policy shall supersede all previous "State" Data Encryption Policies and shall be effective for all state employees, contractors, subcontractors, casual and seasonal employees, and ALL USERS.

4. References

- a. COBIT standards: www.isaca.org/cobit.htm
- b. HIPAA Security Standards: <http://www.hipaadvisory.com/regs/finalsecurity/>
- c. Data Categorization Policy

5. Definitions

- a. **Advanced Encryption Standard (AES)** - The Advanced Encryption Standard (AES) is an encryption standard utilizing the Rijndael specifications for securing sensitive but unclassified material by the federal government agencies.
- b. **Asymmetric Cryptosystem** - A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g. public-key encryption).
- c. **Backup** - Information archived for the purpose of recovering systems and data in the event of a disaster or loss of data.

- d. **Data Encryption Standard (DES)** - The Data Encryption Standard is a symmetric key algorithm adopted by the federal government as a federal standard for protecting sensitive unclassified information. With an effective key length of 56 bits, DES was broken in 1998.
- e. **El Gamal** - The El Gamal algorithm, based on Diffie-Hellman key agreement, is an asymmetric algorithm based on a discrete logarithm problem. The asymmetric algorithm provides encryption and digital signature services.
- f. **File Transfer Protocol (FTP)** - An application layer protocol that uses Transmission Control Protocol (TCP) and telnet services to transfer bulk-data files between machines and hosts.
- g. **Flash drive** - Flash drives, also known as thumb drives or USB drives, are portable storage devices that use flash memory and are very lightweight and small. Flash drives can be used in place of a floppy disk, zip drive disk, or CD.
- h. **IMAP** - (Internet Message Access Protocol) - IMAP is a client/server protocol in which e-mail is received and held for you by your Internet server. You can view just the heading and the sender of the mail and then decide whether to download the mail. You can sync e-mail with your Palm, Blackberry or other portable e-mail device. You can also create and manipulate folders or mailboxes on the server, delete messages etc. IMAP over SSL is also available for secure e-mail transmissions.
- i. **Personal Digital Assistant (PDA)** - A PDA is a small handheld device that combines computing, information storage, telephone, fax and internet.
- j. **RSA** - The RSA algorithm, developed by Rivest, Sharmir and Adleman, can be used for public key encryption and digital signatures. Its security based on the difficulty of factoring large integers.
- k. **SGC** - Server Gated Cryptography (SGC) is Microsoft's name for the entire set of technologies which enable strong encryption when an appropriately configured server encounters an appropriately configured client. This allows the client to connect to your web server at 128 bit, even if they are using 40 or 56 bit browsers.
- l. **Secure Shell (SSH)** - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for security getting access to a remote computer. Both ends of the client/server connection are authenticated using a digital certificate and passwords are encrypted. SSH uses RSA public key cryptography for both connection and authentication.
- m. **SMTP** - Simple Mail Transport Protocol (SMTP) is a protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, which let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.
- n. **Symmetric Cryptosystem** - A method of encryption in which the same key is used for both encryption and decryption of the data.

- o. Telnet** - Telnet is a user command using TCP/IP protocols to access a computer remotely. Using telnet, you can enter commands and they will be executed as if they were being entered directly onto the computer.
- p. Triple DES Encryption** - Triple DES encryption encrypts data with DES algorithm three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits.
- q. Encryption Virtual Private Network (VPN)** - A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

6. Policy

- a.** The following policy applies only to data that is classified by the Data Categorization Policy 05-02 as being confidential or sensitive being stored or transmitted on a public network, including the state network.
- b.** Users accessing data from outside the organizational local area network must encrypt their credentials, including login IDs and passwords, to access such data.
- c.** Data on all portable media and electronic devices, such as laptops, PDAs, flash drives, CDs, DVDs, or any external storage device, including backups, must be encrypted.
- d.** Data shall be encrypted with symmetric crypto algorithms utilizing at least 256 bit key encryption, at a minimum. Asymmetric crypto algorithms keys must be of a length that yields equivalent strength. State key requirements will be reviewed annually and upgraded as technology allows.
- e.** Acceptable methods of 256 bit or higher encryption include, but are not limited to:
 - (i.)** Advanced Encryption Standard (AES)
 - (ii.)** International Data Encryption Algorithm (IDEA)
 - (iii.)** RSA
 - (iv.)** El Gamal
 - (v.)** SSL (secure socket layer)
 - (vi.)** Secure Shell (SSH2)
 - (vii.)** IMAP over SSL
 - (viii.)** SMTP over SSL
- f.** Unacceptable encryption methods include, but are not limited to:
 - (i.)** Data Encryption Standard (DES)
- g.** Encryption shall be used for data transmission such as FTP (file transfer protocol) and Telnet. Methods of acceptable encryption include, but are not limited to, SSH (version 2), third party secure FTP solutions, SSL, and the use of a virtual private network.
- h.** Encryption of data shall only be decrypted by the authorized owner of the data.

- i. It is the responsibility of the owner of the data to disseminate this policy to his/her staff and successors.

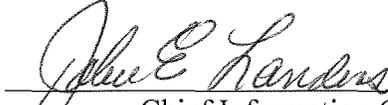
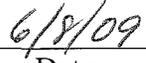
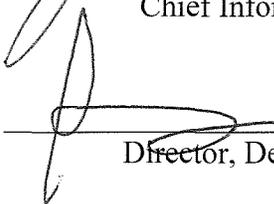
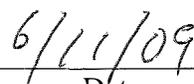
7. Procedures

- a. The State Chief Information Security Officer (CISO) reserves the right to audit for compliance with this standard. Furthermore, the State Chief Security Officer has the right to grant exception or exclusion to any part of this standard. With thirty days written notice, the State CISO reserves the right to update the unacceptable encryption methods listed as defined in Section 6.6.

8. Violations and Disciplinary Actions

- a. A workforce member found in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of the contract, where applicable, may also be considered.

9. Signatures

 _____ Director of Operations	 _____ Date
 _____ Chief Information Officer	 _____ Date
 _____ Director, Department of Administration	 _____ Date