Encryption Policy

Discotheque Inc

November 2020

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity and nonrepudiation of information.

b. This policy applies to all systems, equipment, facilities and information within the scope of the organization's information security program.

c. All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on behalf of the organization having to do with cryptographic systems, algorithms, or keying material are subject to this policy and must comply with it.

2 Background

a. This policy defines the high level objectives and implementation instructions for the organization's use of cryptographic algorithms and keys. It is vital that the organization adopt a standard approach to cryptographic controls across all work centers in order to ensure end-to-end security, while also promoting interoperability. This document defines the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

3 Policy

a. The organization must protect individual systems or information by means of cryptographic controls as defined in Table 3:

Name of System/ Type of Information	Cryptographic Tool	Encryption Algorithm	Key Size
Public Key Infrastructure for Authentication	OpenSSL	AES-256	256-bit key
Data Encryption Keys	OpenSSL	AES-256	256-bit key
Virtual Private Network (VPN) keys	OpenSSL and OpenVPN	AES-256	256-bit key
Website SSL Certificate	OpenSSL, CERT	AES-256	256-bit key

Table 3: Cryptographic Controls

b. Except where otherwise stated, keys must be managed by their owners.

c. Cryptographic keys must be protected against loss, change or destruction by applying appropriate access control mechanisms to prevent unauthorized use and backing up keys on a regular basis.

d. When required, customers of the organization's cloud-based software or platform offering must be able to obtain information regarding:

   i. The cryptographic tools used to protect their information.

   ii. Any capabilities that are available to allow cloud service customers to apply their own cryptographic solutions.

   iii. The identity of the countries where the cryptographic tools are used to store or transfer cloud service customers' data.

e. The use of organizationally-approved encryption must be governed in accordance with the laws of the country, region, or other regulating entity in which users perform their work. Encryption must not be used to violate any laws or regulations including import/export restrictions. The encryption used by the organization conforms to international standards and U.S. import/export requirements, and thus can be used across international boundaries for business purposes.

f. All key management must be performed using software that automatically manages access control, secure storage, backup and rotation of keys. Specifically:

g. The key management service must provide key access to specifically-designated users, with the ability to encrypt/decrypt information and generate data encryption keys.

h. The key management service must provide key administration access to specifically-designated users, with the ability to create, schedule delete, enable/disable rotation, and set usage policies for keys.

i. The key management service must store and backup keys for the entirety of their operational lifetime.

j. The key management service must rotate keys at least once every 12 months.

4 Personally Identifiable Information

Personally Identifiable Information ("PII"), is classified as Confidential Information, which must be encrypted while stored at-rest as well as in-transit. Appropriate encryption technologies must be used to protect PII.

5 Access

The Systems Administrator or their designee shall ensure:

Policies, procedures, scenarios, and processes must identify Confidential Information or PII that must be encrypted to protect against persons or programs that have not been granted access. the organization implements appropriate mechanisms to encrypt and decrypt Confidential Information or PII whenever deemed appropriate. Internal procedures shall specify how the organization transmits sensitive information as well as how often the information is transmitted. When encryption is needed based on data classification to protect Confidential Information or PII during transmission. Procedures shall specify the methods of encryption used to protect the transmission of Confidential Information or PII. Logical user access is managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials) when disk encryption is used rather than file or column-level database encryption.

6 Encryption

The organization's uses software encryption technology to protect Confidential Information or PII. To provide the highest-level security while balancing throughput and response times, encryption key lengths should use current industry standard encryption algorithms for Confidential Information or PII. The use of proprietary encryption algorithms are not allowed unless reviewed by qualified

experts outside of the vendor in question and approved by the organization's management.

6.1 At-Rest

Full disk encryption shall be the method of choice for user devices containing Confidential Information or PII. Confidential Information or PII at rest on computer systems owned by and located within the organization's controlled spaces, devices, and networks should be protected by one or more of the following mechanisms:

1. Disk System Encryption
2. Use of Virtual Private Networks (VPN's) and Firewalls with strict access controls that authenticate the identity of those individuals accessing the Confidential Information or PII
3. Sanitizing, redacting, and/or de-identifying the data requiring protection during storage to prevent unauthorized risk and exposure (e.g., masking or blurring PII)
4. Supplemental compensating or complimentary security controls including complex passwords, and physical isolation/access to the data
5. Strong cryptography on authentication credentials (i.e. passwords/phrases) shall be made unreadable during transmission and storage on all information systems
6. Password protection to be used in combination with all controls including encryption
7. File systems, disks, and tape drives in servers and Storage Area Network (SAN) environments are encrypted using industry standard encryption technology
8. Computer hard drives and other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure upon return for redistribution or disposal

6.2 Portable Devices

Confidential Information or PII cannot be stored on a the organization's portable computing devices.

6.3 In-Transit

In-transit encryption refers to the transmission of data between end-points. The intent of these policies is to ensure that Confidential Information or PII transmitted between companies, across physical networks, or wirelessly is secured

and encrypted in a fashion that protects student Confidential Information or PII from a breach.

The Systems Administrator or their designee shall ensure:

1. Formal transfer policies, protocols, procedures, and controls are implemented to protect the transfer of information through the use of all types of communication and transmission facilities.
2. Users follow the organization's acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting Confidential Information or PII received from non-the organization's staff.
3. Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) are used to safeguard Confidential Information or PII during transmission over open public networks. Such controls include:
4. Only accepting trusted keys and certificates, protocols in use only support secure versions or configurations, and encryption strength is appropriate for the encryption methodology in use.
5. Public networks include but are not limited to the Internet, Wireless technologies, including 802.11, Bluetooth, and cellular technologies.
6. Confidential Information or PII transmitted in e-mail messages are encrypted. Any Confidential Information or PII transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with the organization's must be encrypted or transmitted through an encrypted tunnel (VPN) or point-to-point tunneling protocols (PPTP) that include current transport layer security (TLS) implementations.
7. Wireless (Wi-Fi) transmissions used to access the organization's computing devices or internal networks must be encrypted using current wireless security standard protocols (e.g. RADIUS, WPS private/public keys or other industry standard mechanisms).
8. Encryption or an encrypted/secured channel is required when users access the organization's Confidential Information or PII remotely from a shared network, including connections from a Bluetooth device to a the organization's PDA or cell phone.
9. Secure encrypted transfer of documents and Confidential Information or PII over the internet uses current secure file transfer programs such as "SFTP" (FTP over SSH) and secure copy command (SCP).
10. All non-console administrative access such as browser/web-based management tools is encrypted using SSL based browser technologies using the most current security algorithm.