DFPS Contractor Information Security Standards

Acceptable Use and Prohibitions. Any entity or person who gains access to DFPS confidential information through a properly authorized and current DFPS Agreement, whether formal or informal, must protect that confidential information as required by all applicable standards, agreements, and laws. Any subcontractors performing work required under a DFPS contract on behalf of a DFPS contractor must adhere to the same standards, agreements, and laws.

Article I.

Section 1.01 User Requirements. All DFPS contractors, vendors, and any other person or entity granted access to DFPS information resources must comply with the following standards:

(A) All user computers must be password protected.

(B) Users must either log off or lock access to their workstations before leaving them unattended.

(C) Users must not share their passwords, personal identification numbers (PIN), security tokens (such as Smartcard), or similar information or devices used for identification and authentication to any system or application.

(D) Users of DFPS information resources must protect all account information that can be used to access to any system under DFPS's authority. This includes account identifiers, passwords, personal identification numbers, security tokens, or any other information or device used for user identification or authorization.

(E) Users must not purposely engage in activity that may circumvent computer security measures.

(F) Users of information resources must not engage in any act that would violate the purposes and goals of DFPS as specified in its governing documents, rules, regulations, and procedures.

Section 1.02 Account Management. Account management establishes the standards to create, monitor, control, and remove user accounts. Any entity or person who gains access to DFPS confidential information through a properly authorized and current DFPS Agreement, whether formal or informal, must adhere to these standards for user accounts if they are utilizing or maintaining confidential DFPS data. The account management standard applies equally to all user accounts without regard to their status or category.

(A) All accounts must be identifiable using a unique user ID.

(B) Accounts, other than service accounts, must uniquely identify a specific user.

(C) Account access levels must be reviewed for appropriateness every 12 months, at a minimum.

(D) Upon termination, employee accounts must be disabled.

(E) All access accounts established for contractors, subcontractors, vendors, and/or maintenance accounts must be disabled and deleted immediately upon termination or completion of the contract period.

Section 1.03 Back-up and Disaster Recovery. DFPS requires backups of data and applications to enable the recovery of data in the event of loss or damage due to natural disasters, system disk, and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors. Backups should adhere to these settings if they use or maintain DFPS confidential data on systems that require backup services to recover in the event of data loss.

(A) Backups must be of sufficient frequency and extent to support documented business continuity and disaster recovery plans. Frequency and extent may vary, depending on data classification and owner requirements.

(B) Physical access controls in use at any offsite storage location must meet or exceed the physical access controls defined for the source systems.

(C) Media used in the provision of backup storage must be protected in accordance with the highest level of sensitivity of information being stored.

(D) A success verification process must be implemented for all electronic information backups.

(E) Electronic information backups must be periodically tested to assure recoverability.

(F) At a minimum, stored data must include clearly identifiable labels or coding systems:

(1) System name

(2) Creation date

(3) Sensitivity classification (based on applicable record retention regulations)

(4) Contact information

(G) Offsite storage facilities must be geographically located away from the primary physical location of the information resource so that a single disaster will not destroy the data at both sites.

(H) Confidential DFPS material transmitted over external network connections must be encrypted or otherwise protected as required by rule or law.

Section 1.04 Imaging Devices. Any device that can capture, store, or transmit a still or motion image of any document, person, or environment must have the image-capturing function disabled when the user is operating in any area with access to DFPS information or other restricted DFPS environments. Exemptions to this requirement include dedicated document scanning devices and other equipment designed specifically to capture document images for archival storage.

Section 1.05 Malicious Code. All workstations (desktop, notebook, laptop, systems, or applications) whether connected to the contractor's network, used remotely, or stand-alone, mustuse virus protection software and configurations or a certifiably comparable product.

(A) Users must not disable or bypass virus protection software.

(B) Users must not alter the settings for virus protection software in any manner that will reduce the effectiveness of the software.

(C) Users must enable any automatic updates on antivirus protection software.

Section 1.06 Operating Systems. Any entity or person who gains access to DFPS confidential information through a properly authorized and current DFPS Agreement, whether formal or informal,must ensure all workstations have stable operating system software with appropriate patches and corresponding and complete documentation. Security-related operating system or software application patches must be reviewed and installed periodically, consistent with how critical and vulnerable the resource is.

Section 1.07 Passwords. Passwords must have a minimum length and format as defined by current password guidelines.

(A) Users must not write down passwords and store them near their computers.

(B) Users must not share their passwords with anyone, including when assisting with computer problems, (technicians, Customer Service Center agents, and so on), supervisors, or other employees.

(C) User who doubt their passwords are secure must change them immediately.

(D) Users who suspect their passwords have been compromised should change them immediately.

(E) Users must change new or temporary passwords when they receive them. The network passwords must be set for one-time use to support this policy.

(F) Passwords must have an expiration period of 90 days as defined by current password guidelines.

(G) Stored passwords must be encrypted.

(H) Passwords must:

(1) contain both upper and lower case characters, such as: a-z, A-Z;

(2) have digits and special characters as well as letters, such as: 0-9, !@#$%^&*()_+|~=\`{}[]:";'<>?,./;

(3) be at least eight characters long;

(4) not contain consecutive duplicate characters such as: 99 or BB;

(5) not contain consecutive-count numbers or letters such as: 1234 or ABCD;

(6) not be words found in any dictionary, including slang, dialect, jargon, and so on;

(7) not be based on personal information, names of family, and so on;

(8) not be written down or stored online;

(9) should be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation; and

(10) should never be the same as your user ID.

Section 1.08 Physical Access. The physical access standard establishes rules for granting, controlling, monitoring, and removing physical access to information resource facilities. Each facility must have a documented facility security plan. These standards should be adhered to if DFPS confidential data is being utilized or maintained.

(A) Physical security systems must comply with applicable regulations such as building codes and fire regulations.

(B) Physical access to all restricted facilities or areas must be documented and managed.

(C) Access to information resource facilities must be granted only to authorized personnel whose job responsibilities require access.

(D) The process for granting access, by key card or otherwise, to information resource facilities must include the approval of the designated office or staff person responsible for the facility.

(E) Access to secured facilities and key cards must not be shared or loaned.

(F) Access materials and key cards that are no longer required must be returned to the appropriate building manager, who is the only person authorized to pass the retired card to another user.

(G) Users must report lost or stolen access key cards to the building manager immediately upon becoming aware of the loss.

(H) Secured facilities that allow visitor access must track that access with a sign in log.

(I) Authorized staff must escort visitors to controlled facilities at all times.

(J) Facilities must keep access records, entry and exit logs, and visitor logs based on records retention or other state or federal requirements.

(K) Designated staff must deactivate functional capabilities for an access key card upon termination of need.

Section 1.09 Portable / Remote Computing. Any entity or person who gains access to DFPS confidential information through a properly authorized and current DFPS Agreement, whether formal or informal, must not store confidential data on portable computing devices. In the event that there is no alternative to local storage, users must encrypt all confidential data. Any entity or person who gains access to DFPS confidential information through a properly authorized and current DFPS Agreement, whether formal or informal, must maintain active antivirus protection and appropriate security patch levels for portable computing devices equivalent to those applied to any other computing device.

Section 1.10 Removable Media. The security standard for removable media establishes those rules necessary to protect the data of DFPS.

(A) Sensitive, confidential and restricted personal information data that is stored on removable media must be encrypted.

(B) All removable media must be scanned for malicious code content before use on any systems or networks.

(C) These devices include, but are not limited to:

(1) diskettes, tapes, and compact disks (CD/DVDs);

(2) memory cards or sticks used in various portable digital devices;

(3) drive memory devices such as Firewire and USB flash, key, pen, and thumb; and

(4) portable mass storage devices.

Section 1.11 Vendor Access. DFPS has established its standard for vendor access to assure the security of DFPS information resource assets involving vendor interaction. Vendors must comply with all applicable DFPS policies, practices, standards, and agreements, including those related to:

(A) acceptable use;

(B) password;

(C) auditing;

(D) safety;

(E) security; and

(F) software licensing.

Section 1.12 Any entity or person who gains access to DFPS confidential information through a properly authorized and current DFPS Agreement, whether formal or informal, must ensure that confidential and sensitive personal data at rest on computer systems is protected by at least one of the following:

(A) Encryption

(B) Firewalls with strict access controls that authenticate the identity of those individuals accessing systems data

(C) Sanitization of the data requiring protection during storage to prevent unauthorized exposure (such as truncating last four digits of a Primary Account Number)

(D) Other compensating controls including complex passwords or physical isolation or access

(E) Password protection used in combination with all controls including encryption

Section 1.13 Situations where DFPS Requires Encryption. Password protection alone is not an acceptable alternative to protecting confidential and sensitive personal data. DFPS requires the use of encryption in the following circumstances:

(A) Confidential and sensitive personal information back-up data must be protected using encryption methodologies.

(B) Removable media including CDs, DVDs, floppy disks, backup tapes, and USB memory drives that contain confidential or sensitive personal information must be encrypted and stored in a secure, locked location.

(C) Confidential or sensitive personal information transmitted as an e-mail message must be encrypted.