SECTION II

REQUIREMENT 1.2 TO 1.2.3

FIREWALL AND ROUTER CONFIGURATIONS POLICY AND PROCEDURES

1.2 TO 1.2.3 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures concerning firewall and router configurations to the cardholder data environment. This policy is to be implemented immediately. It will be evaluated on an *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

1.2 TO 1.2.3 POLICY

Surplus Property will have the Department of Technology Services (DTS) ensure that the firewall and router configurations policy adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. Specifically, that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.
- Secure and synchronize router configuration files. Specifically, that running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.
- Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

1.2 TO 1.2.3 ADDITIONAL SUPPORTING DOCUMENTATION

Please Note: *If your organization would like to comment on and/or list any other supporting documentation that would assist with compliance with Requirement 1.2 to 1.2.3, then please do*

1.2 TO 1.2.3 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 1.3.1 TO 1.3.6

DMZ CONFIGURATION AND INTERNET ACCESS TO THE CARDHOLDER DATA ENVIRONMENT POLICY AND PROCEDURES

1.3.1 TO 1.3.6 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures concerning DMZ configuration and Internet access to the cardholder data environment. This policy is to be implemented immediately. It will be evaluated on an *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

1.3.1 TO 1.3.6 POLICY

Surplus Property will have the Department of Technology Services (DTS) ensure that the DMZ configuration and Internet access to the cardholder data environment policy adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- Ensure that a Demilitarized Zone (DMZ) is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports.
- Ensure that inbound traffic is limited to IP addresses within the DMZ.
- Ensure that direct connections, inbound or outbound, are not allowed for traffic between the Internet and the cardholder data environment.
- Ensure that internal addresses cannot pass from the Internet into the DMZ.
- Ensure that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.

- Ensure that the firewall(s) perform Stateful Packet Inspection (SPI).

The exposure of cardholder data environment system components to direct public Internet access poses obvious security risks by allowing untrusted parties to make direct connections to an environment containing privileged information. The prohibition of direct public Internet access to system components within cardholder data environments helps to ensure that sensitive data, as well as the architecture where sensitive data reside, are insulated from external threats seeking to exploit information or resources.

1.3.1 TO 1.3.6 PROCEDURE

In order to ensure that the DMZ configuration and Internet access to the cardholder data environment adhere to Payment Card Industry Data Security Standards (PCI DSS) requirements, complete the DMZ Configuration Checklist and to answer all section as needed.

1.3.1 TO 1.3.6 ADDITIONAL SUPPORTING DOCUMENTATION

Please Note: *If your organization would like to comment on and/or list any other supporting documentation that would assist with compliance with Requirement 1.3.1 to 1.3.6, then please do so. For example, your processes and procedures for firewall and router configurations for protecting the car may be that of opening up an actual change ticket or support ticket, or even signing off on an internal checklist. If so, please discuss here. Additionally, your organization may have other supporting documents that discuss reviewing firewalls and routers for security reasons. If so, please discuss as needed. Listed below is a simple example of how best to illustrate this in a table format. You can use the table, modify or simply delete it.*

ADDITIONAL SUPPORTING DOCUMENTATION

Document Name	Description of Document	Date Last Updated
?	*?*	*?*
?	*?*	*?*
?	*?*	*?*
?	*?*	*?*
?	*?*	*?*

1.3.1 TO 1.3.6 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

CHECKLIST 1.3.1 TO 1.3.6

DMZ CONFIGURATION CHECKLIST

Note: This is a comprehensive checklist to be used for ensuring your network topology is configured in accordance with PCI DSS requirements.

General Information				
Name of Individual Performing the ***DMZ Configuration*** Review				
Last Name	**First Name**	**Middle Name**	**Title**	**Date of Review**
King	Timothy	T.	Technical Support Specialist III	**12/18/13**
Additional Information				
Department	**Division**	**Office**	**Immediate Supervisor**	**Secondary Supervisor**
DTS			Aaron Jeter	
Physical Location of DMZ Configuration Review				
Street Address and Suite #	**City**	**State**	**ZIP**	**Country**
14717 South Minuteman Dr	**Draper**	**Utah**	**84020**	

Signature of Individual Performing the Review	**Signature of Reviewing Supervisor or Authority**

Listing of system components that were appropriately configured for establishing a DMZ along with prohibiting direct access to the cardholder data environment	
(1)Cisco ASA 5520	**(5)**
(2)Cisco Catalyst 6509 layer 3 switch	**(6)**
(3) Cisco 7206VXR router	**(7)**
(4)	**(8)**

Req. 1.3.1: Have processes and procedures been undertaken for ensuring that a Demilitarized Zone (DMZ) is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports?	**Yes**	**No**
Notes/Comments:		
Req. 1.3.2: Have processes and procedures been undertaken for ensuring that inbound traffic is limited to IP addresses within the DMZ?	**Yes**	**No**
Notes/Comments: Per Rick Johnson, DTS Security		

Req. 1.3.3: Have processes and procedures been undertaken for ensuring that direct connections, inbound or outbound, are not allowed for traffic between the Internet and the cardholder data environment?	**Yes**	**No**
Notes/Comments: Per Rick Johnson, DTS Security		
Req. 1.3.4: Have processes and procedures been undertaken for ensuring that internal addresses cannot pass from the Internet into the DMZ?	**Yes**	**No**
Notes/Comments: Per Rick Johnson, DTS Security		
Req. 1.3.5: Have processes and procedures been undertaken for ensuring that outbound traffic from the cardholder data environment to the Internet is explicitly authorized?	**Yes**	**No**
Notes/Comments: Per Rick Johnson, DTS Security		
Req. 1.3.6: Have processes and procedures been undertaken for ensuring that the firewall(s) perform Stateful Packet Inspection (SPI)?	**Yes**	**No**
Notes/Comments: Per Rick Johnson, DTS Security		

REQUIREMENT 2.1 TO 2.1.1

CHANGING OF VENDOR DEFAULT SETTINGS POLICY AND PROCEDURES

2.1 TO 2.1.1 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures for the changing of vendor default settings for all system components and wireless environments. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding *Surplus Property* 's needs and goals.

2.1. TO 2.1.1 POLICY

Surplus Property will have the Department of Technology Services (DTS) ensure that the changing of vendor default settings for all system components and wireless environments adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.2):

- Vendor-supplied defaults, such as passwords and simple network management protocol (SNMP) community strings, are changed before installing a system on the network.
- All unnecessary accounts are eliminated before installing a system on the network.
- Encryption keys are changed from the default settings at installation; they are also changed anytime anyone with knowledge of the keys leaves the company or changes positions.
- The default SNMP community strings on wireless devices are changed.
- The default passwords and passphrases on access points are changed.
- All firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.
- When applicable, other security-related wireless vendor defaults are changed.
- Adhere to additional protocols as needed to ensure overall wireless network security.

2.1 TO 2.1.1 PROCEDURE

Surplus Property will have the Department of Technology Services (DTS) develop and implemented a comprehensive program regarding changing of vendor default settings for all system components and wireless environments and additional protocols as needed for ensuring the overall security for wireless networks, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *DTS* for ensuring the vendor default settings are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by *Surplus Property*. DTS follows NIST guidelines and has policies and procedures documented concerning these areas. Further documentation here is not considered necessary.

2.1 TO 2.1.1 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 2.2 TO 2.3

CONFIGURATION STANDARDS FOR ALL SYSTEM COMPONENTS POLICY AND PROCEDURES

2.2 TO 2.3 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Department of Technology Services (DTS)* has established a formal policy and supporting procedures for developing configuration standards for system components that are consistent with industry-accepted hardening standards. This process will be conducted by authorized personnel with the appropriate technical knowledge and skill sets needed to undertake this activity. The term, *System Components,* is defined as any network component, server or application included in or connected to the cardholder data environment.

2.2 TO 2.3 POLICY

Department of Technology Services (DTS) will develop configuration standards for system components utilizing industry-accepted hardening standards for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. The list of industry-leading security standards, benchmarks and frameworks to utilize includes, but is not limited to, the following (PCI DSS Requirements and Security Assessment Procedures, Version 3.2):

- SysAdmin Audit Network Security (SANS) http://www.sans.org
- National Institute of Standards and Technology (NIST) http://www.nist.gov
- Center for Internet Security (CIS) http://www.cisecurity.org
- International Organization for Standardization (ISO)
- Vendor-specific tools and checklists, along with general setup and hardening procedures

Additionally, when configuring system components within the cardholder environment the following conditions must apply in order to ensure further compliance with the Payment Card Industry (PCI) Data Security Standards (DSS) Initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.2):

- System configuration standards are updated as new vulnerability issues are identified.
- System configuration standards are applied when new systems are configured.
- Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server.
- When utilizing virtualization, only one primary function per virtual system component is allowed.
- Enable only necessary and secure services, protocols, daemons and other services for the function of the system.
- Configure system security parameters to prevent misuse at all times and on all system components.
- Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers.
- Enabled functions on all system components are documented, they support secure configuration, and documented functionality exists for all system components.
- Encrypt all non-console administrative access by using strong cryptography at all times.

2.2 TO 2.3 PROCEDURE

Department of Technology Services (DTS) has developed and implemented a comprehensive program regarding configuration standards for all system components, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *DTS* in order to ensure that configuration standards initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by *Surplus Property*.

SYSTEM CONFIGURATION STANDARDS

When deploying or making modifications to any system component within the cardholder environment, authorized personnel will utilize the previously mentioned industry-leading

security standards for this particular activity and any other industry-leading security frameworks considered acceptable by *DTS*.

ONLY ONE PRIMARY FUNCTION PER SERVER

When deploying or making modifications to system components, there is to be only one primary function per server so as not to require different security levels on any one given server. But more importantly, having more than one primary function per server could possibly result in multiple systems failing and rendering other critical infrastructure inoperable. This could severely impact all technology platforms within *DTS*. As such, all servers, both physical and virtual, will operate with one primary function only.

SYSTEM CONFIGURATION AND HARDENING PROCEDURES

When deploying or making modifications to system components, authorized IT personnel are to use only approved configuration documentation, which provides specific guidelines on the processes and procedures to undertake. All hardening procedures are to result in the reduction of the system component becoming vulnerable to any number of security issues, both internal and external. While ease-of-use and flexibility of the systems are important to system administrators and other IT personnel, the security of the system components themselves are the single most important factor when hardening procedures are undertaken.

NON-CONSOLE ADMINISTRATIVE ACCESS

Many system components within the cardholder data environment are accessed through a non-console administrative function; thus, they must ensure that strong cryptography is in place at all times. The following is a list of protocol, secure data transmission elements and tools that are used for accessing various system components:

- Secure Shell (SSH)
- Virtual Private Network (VPN)
- Secure Socket Layer (SSL) | Transport Layer Security (TLS)

2.2 TO 2.3 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 4.1

THE USE OF STRONG CRYPTOGRAPHY POLICY AND PROCEDURES

4.1 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Department of Technology Services (DTS)* has established a formal policy and supporting procedures concerning the use of strong cryptography. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

4.1 POLICY

Department of Technology Services (DTS) will ensure that the Use of Strong Cryptography Policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.2):

- Security protocols are utilized and in place wherever cardholder data is transmitted or received over open, public networks.
- Strong cryptography is used during data transmission, and that only trusted keys and/or certificates are accepted.
- The applicable security protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.
- Proper encryption strength is implemented for the encryption methodology in use.
- For wireless networks transmitting cardholder data or connected to the cardholder data environment, industry best practices are used to implement strong encryption for authentication and transmission.

4.1 PROCEDURE

The procedures, which ensure that the use of strong cryptography policy adheres to the requirements as set forth for Payment Card Industry Data Security Standards (PCI DSS) compliance, require observance of the aforementioned policies, the table below to be completed and its columns completely answered.

Type of Cryptography Used	Primary Purpose	Is Protocol Used for Sending and Receiving of Primary Account Numbers (PAN)?
HTTPS	*Encryption*	*Yes*
SSL TLS (On Server)	*Certificate*	*Yes*

4.1 Responsibility for Policy Maintenance

The *Department of Technology Services (DTS)* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 4.2

UNENCRYPTED PRIMARY ACCOUNT NUMBERS (PAN) POLICY AND PROCEDURES

4.2 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures concerning unencrypted Primary Account Numbers (PAN) that are not to be sent via end-user messaging technologies. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

4.2 POLICY

Surplus Property will ensure that unencrypted Primary Account Numbers (PAN) are not sent via end-user messaging technologies and that they adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.2):

- Primary Account Numbers (PAN) will not be sent via unencrypted email.
- Primary Account Numbers (PAN) will not be sent via an instant messaging protocol.
- Primary Account Numbers (PAN) will not be sent via a chat protocol or forum sessions.
- If for any reason, Primary Account Numbers (PAN) must be sent via end-user messaging technologies, they are to be sent using strong encryption, rendering the PAN unreadable.

4.2 PROCEDURE

The procedures, which ensure that the unencrypted Primary Account Numbers (PAN) policy adheres to the requirements as set forth for Payment Card Industry Data Security Standards (PCI DSS) compliance, require observance of the aforementioned policies, the table below to be completed and its columns regarding unencrypted PANs to be answered.

End-User Messaging Technologies Currently Used	Primary Purpose and Use of Protocol	Is Protocol Used for Sending and Receiving of Primary Account Numbers (PAN)?

Unencrypted Email	*Business Email*	*No*
AOL Instant Messaging	*Communicate internally with employees*	*No*
Yahoo Instant Messaging	*Communicate internally with employees*	*No*
Third-Party Chat Software	*Communicate with prospective clients*	*No*
Client forum Sessions built into the Content Management System (CMS)	*Communicate with clients*	*No*
Encrypted Email	*Communicate with clients*	*Only if absolutely necessary and no other means are available.*

4.2 Responsibility for Policy Maintenance

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Requirement 5.1 to 5.2

Anti-Virus Policy and Procedures

5.1 TO 5.2 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *[com Department of Technology Services (DTS)* has established a formal policy and supporting procedures concerning anti-virus. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

5.1 TO 5.2 POLICY

Department of Technology Services will ensure that the Anti-Virus policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- A licensed anti-virus software must be utilized for all computer and system components (any network component, server or application included in or connected to the cardholder data environment) within the cardholder environment and for all computers not directly associated with the cardholder environment.
- The licensed anti-virus software utilized must be the most current version available.
- All computers and system components within the cardholder environment must have standard, supported anti-virus software installed.
- The anti-virus software must be active, must be scheduled to perform virus checks at regular intervals and must have its virus definition and all other associated software files kept current.
- The anti-virus software must be enabled for automatic updates and periodic scans.
- All computers not directly associated with the cardholder environment must have standard, supported anti-virus software installed.
- The anti-virus software for all computers not directly associated with the cardholder environment must also be active, scheduled to perform virus checks at regular intervals and must have its virus definitions and all other associated software files kept current.
- No user shall disable or tamper with the configuration of anti-virus software installed on their respective computer.
- Employees who allow non-company employees to attach workstations (desktops or laptops) to the company network are responsible for ensuring that those workstations are running anti-virus software and that a current virus signature is installed.
- Employees who attach workstations to the company network are responsible for ensuring that those workstations are running anti-virus software and that a current virus signature is installed.
- Never open any emails that are from an unknown or suspicious source.
- Never open any email attachments from an unknown or suspicious source.

5.1 to 5.2 Procedure

The procedure, which ensures that the Anti-Virus policy adheres to the following Payment Card Industry Data Security Standards (PCI DSS) compliance requirements, calls for observance of the aforementioned policies, the table below to be completed and its columns regarding anti-virus measures to be answered.

Anti-Virus Software Utilized

[Please discuss in detail the anti-virus product your organization utilizes, the current version used, the general system settings that are in place for ensuring that the software is enabled for automatic updates and scans and that virus definition files are continually updated, etc. Also, please complete the table below.]

Anti-Virus Attributes for the Cardholder Data Environment

Computers and System Components within Cardholder Data Environment that Utilize Anti-Virus	Anti-Virus Product Utilized	Current Version of Anti-Virus Product being Utilized	Virus Definition files Up-to-Date as Needed
All company-owned laptops and netbooks	*Symantec Endpoint Protection*	*12.1.6*	*Yes*
All employee-owned laptops and netbooks	*Symantec Endpoint Protection*	*12.1.6*	*Yes*
DBAMA001-Database server with Microsoft Windows Server 2008 O/S	*Symantec Endpoint Protection*	*12.1.6*	*Yes*

5.1 to 5.2 Responsibility for Policy Maintenance

The *Department of Technology Services (DTS)* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 6.1

SECURITY PATCH MANAGEMENT INSTALLATION POLICY AND PROCEDURES

6.1 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Department of Technology Services (DTS)* has established a formal policy and supporting procedures concerning security patch management. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

6.1 POLICY

Security patch management (patch management) has become a critical security issue due in large part to the exploitation of information technology systems from numerous external and internal sources. Consequently, all system components directly associated with the cardholder data environment must be securely hardened and configured with all necessary and appropriate patches and system updates for preventing the exploitation or disruption of mission-critical services. Similarly, all IT resources not directly associated with the cardholder data environment must also be securely hardened and configured with all necessary and appropriate patches and system updates in order to prevent the exploitation or disruption of mission-critical services.

In accordance with best practices for security patch management, the subsequent three (3) security concerns will be highlighted throughout the Security Patch Management policy. They are as follows (NIST, n.d.):

- **Vulnerabilities**: Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the system components directly associated with the cardholder data environment or any other IT resources

- **Remediation:** The three (3) primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting and (3) removal of affected software.
- **Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Common examples are scripts, worms, viruses and Trojan horses.

Failure to keep system components and other IT resources patched securely and on a consistent basis can cause unwanted damage to all environments directly associated with the cardholder environment. This includes but is not limited to the following:

- Network devices and all supporting hardware and protocols
- Operating systems within the development and production environments
- Applications within the development and production environments
- Any other mission-critical resources within the cardholder data environment that require patches and security updates for daily operations

Additionally, a Security Patch Management Program (SPMP) is to be implemented, which consists of the following initiatives:

- A formalized Security Patch Management Program employee, complete with his/her roles and responsibilities
- Comprehensive inventory of all system components directly associated with the cardholder environment
- Comprehensive inventory of all other IT resources not directly associated with the cardholder environment
- Subscribing to industry-leading security sources, additional supporting resources for vulnerability announcements and other security patch management alerts and issues
- Procedures for establishing a risk ranking regarding security patch management. This will include but is not limited to (1) the significance of the threat, (2) the existence and overall threat of the exploitation and (3) the risks involved in applying security patch management procedures (its effect on other systems, resources available and resource constraints).
- The creation of a database of remediation activities that needs to be applied
- Test procedures for testing patches regarding remediation
- Procedures for the deployment, distribution and implementation of patches and other related security-hardening procedures
- Procedures for verifying successful implementation of patches and other related security-hardening procedures

6.1 Procedure

Department of Technology Services (DTS) has developed and implemented a comprehensive program regarding security patch management, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *[Department of Technology Services (DTS)* for ensuring the Security Patch Management Program (SPMP) initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources.

Security Patch Management Program Employee

This individual will be responsible for coordinating, facilitating and undertaking all necessary activities regarding security patch management policies and procedures. Additionally, this individual will have the necessary information technology and security expertise to successfully execute all steps as required. Specifically, this individual will have a strong working knowledge of vulnerability and patch management, as well as system administration, intrusion detection and firewall management.

Security Patch Management Program Employee

Name	Title	Contact Information
Desktop Support	*Desktop Support*	*DTS Ticket*

Comprehensive Inventory of All System Components Directly Associated with Cardholder Environment

The following table includes all system components that are directly associated with the cardholder environment. These system components are to be listed by network devices, operating systems, applications and any other system components as needed.

*System Components	Host Name	Physical Location	Owner of System Components	Primary Use in Cardholder Data Environment
Point of Sale Unit	*168.178.64.42*	*Surplus Property*	*State of Utah*	*Processing Payment(s)*
iPad	*N/A*	*Surplus Property*	*State of Utah*	*Processing Payment(s)*

***currently using POS Verifone VX520 S/N 289267775**

Industry-Leading Security Sources and Additional Supporting Resources

Various external security sources and resources are utilized to ensure that *Surplus Property* maintains awareness of security threats, vulnerabilities and what respective patches, security upgrades and protocols are available.

Currently, *Department of Technology Services (DTS)* subscribes to the following types of security sources and resources (NIST, n.d.):

- Vendor websites and email alerts
- Vendor mailing lists, newsletters and additional support channels for patches and security
- Third-party websites and email alerts
- Third-party mailing lists
- Online forums and discussion panels
- Conferences, seminars and trade shows

Listed below are the specific security resources and sources to which *[company name]* subscribes for patch management, alerts, security and support as applicable:

Online Resources for Patch Management, Alerts, Security and Support, As Applicable

Vendor/Provider and Type of System	Website	Other
CISCO	**http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml** DTS Policy 2.3.10	*Security Advisory Alert Board*
IBM AIX	**http://www-03.ibm.com/systems/power/software/aix/service.html**	*AIX support and alert website*
Microsoft	**http://technet.microsoft.com/en-us/wsus/default.aspx**	*Windows Server Update Services (WSUS)*
Oracle	**http://www.oracle.com/technology/deploy/security/alerts.htm**	*Critical Patch*

		Updates and Security Alerts
Apache	**http://www.apache.org/dist/httpd/patches**	*Official Patches for Apache*

Please note: This is just a sample used to illustrate how this section should be completed. For an in-depth listing of all vendors, providers, their products and respective websites, please view Appendix D from the following URL: http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf. *Additionally, please add any other vendors that you use.*

RISK RANKING FOR SECURITY PATCH MANAGEMENT

A Risk Ranking matrix will be established regarding security patch management. Specifically, system components and other associated IT resources will be given a risk ranking pertaining to the importance of security patch management activities to be undertaken.

In accordance with NIST SP 800-30, *Department of Technology Services (DTS)* will adhere to the following definitions regarding risks that are related to all system components within the cardholder environment and any other IT resources.

- **High:** The threat source is highly motivated and sufficiently capable; controls to prevent the vulnerability from being exercised are ineffective.
- **Medium:** The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- **Low:** The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

RISK RANKING TABLE

Critical Security Threats	Response Mechanisms to Initiate	Priority Level 1 (High)	Priority Level 2 (Medium)	Priority Level 3 (Low)
Vendor Patches and security updates defined as "high," "critical" or "urgent" for all system components and other IT resources affected	*Please discuss your response mechanisms for these types of security threats.*	*X*		

by threat				
Vendor Patches and security updates defined as "medium," "moderate" or "important" for all system components and other IT resources affected by threat	*Please discuss your response mechanisms for these types of security threats.*		*X*	
Vendor Patches and security updates defined as "low," "non-essential" or "non-urgent" for all system components and other IT resources affected by threat	*Please discuss your response mechanisms for these types of security threats.*			*X*
Security alerts from SANS, CERT, NIST, CIS and all other industry-leading associations	*Assign risk accordingly based on each individual threat.*			
Recommendations from all other industry-leading security sources (online forums, email subscriptions to security forums, etc.) regarding threats	*Assign risk accordingly based on each individual threat.*			

Additionally, the Security Patch Management Program employee will also be responsible for the following critical activities:

- Being aware of all known threats or vulnerabilities that could significantly impact system components within the cardholder data environment and any other IT resources. This requires consistent oversight and management of all online resources used for security patch management as previously described.
- Having a strong technical and business understanding of all critical systems within the organization's IT infrastructure, as well as knowing which systems are essential for day-to-day operations
- Having response mechanisms and procedures in place to immediately report the scope of the exploitation (systems affected), the impact to the IT infrastructure as a whole and

which remediation activities and plan of action initiatives are already available to the management in the event of network exploitation.

Database of Remediation Activities that Need to be Applied

The database for remediation activities will consist of listing the relevant Uniform Resource Locators (URL) for each patch and specific advice and any other comments deemed critical to the patch itself. Additionally, the Security Patch Management Program employee will be responsible for keeping the database accurate and relevant.

System Components within Cardholder Data Environment and other IT Resources	Uniform Resource Locator (URL) for Patch	Notes/Comments
Oracle	http://www.oracle.com/technology/deploy/security/alerts.htm#CriticalPatchUpdates	*Online board and listing for Oracle products and their respective patches*
Microsoft	http://www.microsoft.com/security/updates/bulletins/default.aspx	*Online board and listing for Microsoft products and their respective patches*

Test Procedures for Testing Patches Regarding Remediation

Security patch management testing procedures must be observed to ensure the authenticity of the patch or any other security upgrades before they are released to day-to-day operations. The following testing procedures are to be adhered to (NIST, n.d.):

- An acceptable test environment (non-production systems) will be determined and utilized, if necessary, for each and every patch and security upgrade implemented by the SPMP employee.
- For vendors providing patches, the authenticity of the downloaded patch will need to be verified. This verification process will be determined as needed for patches and security upgrades.
- A virus scan is to be run on all patches before installation.
- Determine *patch dependency* or any other issues that may result in the installation of the patch. Would the installation of the new patch disable another? Are other patches uninstalled when the new patch is installed?

Procedures for the Distribution, Deployment and Implementation of Patches and other Related Security-Hardening Procedures

All patches and security updates are to be pushed out in a formalized and secure manner, with all critical patches installed within one (1) month of release from a vendor or other approved third party. This includes using the following:

- Enterprise Patch Management software
- Secured email lists sent to authorized personnel
- Secure internal web source for retrieving patches sent out by the SPMP employee

PROCEDURES FOR VERIFYING SUCCESSFUL IMPLEMENTATION OF PATCHES AND OTHER RELATED SECURITY-HARDENING PROCEDURES

It is the responsibility of the SPMP employee to verify the successful implementation of all patches and security upgrades to *Department of Technology Services (DTS's)* IT infrastructure. These activities will consist of, but are not limited to, the following:

- Verifying that the files have been changed as stated in the vendor's documentation to reflect the updates as needed
- Verifying whether the recommended patches and security updates were installed properly by reviewing patch logs

6.1 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Department of Technology Services (DTS)* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 7.1 TO 7.1.2

DATA CONTROL & ACCESS CONTROL POLICIES AND PROCEDURES

7.1 TO 7.1.2 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures concerning data control and access control. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

7.1 TO 7.1.2 POLICY

Surplus Property will ensure that the Data Control & Access Control policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- Access rights for privileged users are restricted to the least privileges necessary to perform job responsibilities.
- Privileges are assigned to individuals based on job classification and function, such as Role-Based Access Control (RBAC).
- Access control systems are in place on all system components.
- Access control systems are configured to enforce privileges assigned to individuals based on job classification and function.

7.1 TO 7.1.2 PROCEDURE

Surplus Property has developed and implemented a comprehensive Data Control & Access Control program, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *Surplus Property* to ensure that the data control and access control initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by *Surplus Property.*

RESTRICTING ACCESS TO FEWEST PRIVILEGES NECESSARY FOR JOB FUNCTIONS AND RBAC MEASURES

Surplus Property adheres to the concept of Role-Based Access Control (RBAC). RBAC results in users being assigned privileges based on a job classification or function. In short, permissions to perform certain operations are assigned to specific roles, resulting in users acquiring the permissions to perform particular system functions on system components and other I.T resources within the organization. Therefore, privileges to these system components and other IT resources are never to be assigned based on a specific employee's demands, requests or preferences.

PRIMARY ELEMENTS OF ROLE-BASED ACCESS CONTROL (RBAC)

As defined by the National Institute of Standards and Technology (NIST), a comprehensive and mature RBAC architecture consists of the following elements: user, role, permissions/operations and objects.

PERMISSIONS/OPERATIONS AND OBJECTS (NIST, n.d.)

- **User:** The user is any entity that wishes to access data. Generally speaking, a user can be considered an employee who is attempting to gain access to a specific resource or object, such as system components within the cardholder data environment. A user

can also be a mechanism or another entity attempting to gain access to a specific resource or object.

- **Role:** A role can be viewed as permissions that are assigned to a user based on a specific job function within the *Surplus Property* environment for system components within the cardholder data environment and other IT resources. Many times a user may have more than one assigned role, which is based on the needs and security requirements of *Surplus Property*.

- **Permissions/Operations:** Roles are assigned various permissions and operations, which can be considered specific and very diminutive functions.

- **Objects:** Objects can be considered any system component within the cardholder data environment that contains information that requires access by that user. These objects can vary widely from network systems, operating systems, applications, databases and any other components within these devices, or from a subset of them that requires access.

LASTLY, RBAC PRIMARY RULES CONSIST OF THE FOLLOWING (NIST, n.d.)

- **Role Assignment:** Where a subject can execute a transaction only if the subject has been selected or been assigned a role
- **Role Authorization:** Where a subject's active role must be authorized for that subject
- **Transaction Authorization:** Where a subject can execute a transaction only if the transaction is authorized for the subject's active role

Surplus Property will adhere to the above RBAC rules to restrict access to the fewest privileges necessary to perform job functions.

7.1 TO 7.1.2 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 9.6

PHYSICALLY SECURE ALL MEDIA POLICY AND PROCEDURES

9.6 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures concerning physically securing all media. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

9.6 POLICY

Surplus Property will ensure that the Physically Secure All Media policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- Procedures are in place for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).

9.6 PROCEDURE

Surplus Property has developed and implemented a comprehensive program concerning physically securing all media, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *Surplus Property* to ensure that the physically securing of all media initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by *Surplus Property*.

Devices are located in a secure environment accessible by card key entry and are limited to personal that need to perform their job function.

9.6 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 9.10

PERIODIC MEDIA DESTRUCTION POLICY AND PROCEDURES

9.10 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures concerning periodic media destruction. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

9.10 POLICY

Surplus Property will ensure that the Periodic Media Destruction policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- Once the maximum retention period has been allotted for cardholder data, it must be removed from all electronic media, and any hardcopy edition must be disposed of accordingly.
- All hardcopy materials are to be cross-shredded, incinerated or pulped, such that there is reasonable assurance the hardcopy materials cannot be reconstructed.
- Storage containers for shredding hardcopy materials are to be secured at all times, with appropriate physical controls such as locks on the storage bins.
- Cardholder data on electronic media are to be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion or otherwise physically destroying the media such as degaussing.

9.10 PROCEDURE

Surplus Property has developed and implemented a comprehensive program concerning periodic media destruction, which encompasses the following categories and supporting activities. These policy directives will be fully enforced by *Surplus Property* for ensuring the periodic media destruction initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by the organization.

DESTRUCTION OF HARDCOPY MATERIALS

Once the maximum retention period has been allotted for cardholder data, it must be removed from all electronic media, and any hardcopy edition must be disposed of accordingly. Thus, hardcopy materials containing cardholder data will be destroyed via cross-shredding, incineration or pulping. Additionally, storage containers for shredding hardcopy materials are secured at all times, with locks on the storage bins themselves. Lastly, the storage bins are located in the following areas of the facility so that employees have visible access for disposing of hardcopy materials: When done a contracted secure shredding vendor under contract with State Purchasing will be used (Current contract PA376)

DESTRUCTION OF ELECTRONIC MEDIA

Electronic media that contain cardholder data and that are no longer in use will be destroyed using the following procedures:

- A secure wipe program in accordance with industry-accepted standards for secure deletion (i.e., degaussing)
- Disintegration
- Shredding (disk grinding device)
- Incineration by a licensed incinerator
- Pulverization

When done a contracted secure shredding vendor under contract with State Purchasing will be used (Current contract MA2029)

9.10 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Surplus Property* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 11.1

WIRELESS ACCESS POINTS CHECKLIST

General Information **(Incident Ticket INC0128893 2/3/2014)**				
Name of Individual Performing the ***Wireless Access Points*** Review				
Last Name	**First Name**	**Middle Name**	**Title**	**Date of Review**

Additional Information				
Department	**Division**	**Office**	**Immediate Supervisor**	**Secondary Supervisor**
Physical Location of Wireless Access Points Review				
Street Address and Suite #	**City**	**State**	**ZIP**	**Country**

Signature of Individual Performing the Review	**Signature of Reviewing Supervisor or Authority**
Description of Primary Tool used for Detecting Wireless Access Points *Open-source tool designed to discover wireless access points and wireless clients*	**Description of any secondary or supporting Tool(s) used for Detecting Wireless Access Points**

Were procedures undertaken for detecting and identifying any unauthorized Wireless Access Points, such as the following?		
(1) WLAN cards inserted into system components?	**Yes**	**No**
(2) Portable wireless devices connected to system components, such as USB devices?	**Yes**	**No**
(3) Wireless devices attached to a network port or network device?	**Yes**	**No**
(4) Is automated monitoring utilized for any wireless devices and/or systems?	**Yes**	**No**
(5) If automated monitoring is utilized, have the wireless devices and/or systems been configured to allow for alert generation?	**Yes**	**No**
(6) Were any Incident Response procedures enacted due to exceptions or security concerns identified during the Wireless Access Points Review?	**Yes**	**No**
If yes, please detail what Incident Response Procedures were enacted:		
Notes/Comments		

REQUIREMENT 12.1

INFORMATION SECURITY POLICY

Note: Requirement 12.1 states the following:

"Examine the Information Security policy and verify that the policy is published and disseminated to all relevant system users (including vendors and business partners)" (Security Standards Council, Version 3.2).

Please note that this comprehensive document is included in section III.

REQUIREMENT 12.3

**USAGE POLICIES AND PROCEDURES

12.3 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Department of Technology Services (DTS)* has established a formal policy and supporting procedures concerning usage policies for critical employee-facing technologies. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

Usage policies and the supporting Acceptable Uses policies (commonly known as Acceptable Usage Policies [AUP]) are known as the policies and supporting procedures that define proper use of critical employee-facing technologies within an organization. These technologies generally consist of the following system components and additional IT resources deemed critical by any organization:

- Network devices
- Operating systems
- Applications
- Databases
- Remote access technologies
- Wireless technologies
- Removable electronic media
- Desktops
- Laptops
- Personal Data Assistants (PDA)
- Cell phone
- Internet use
- Email use

- Blogging
- Social media forums

12.3 POLICY

Department of Technology Services (DTS) will ensure that the usage policies for critical employee-facing technologies will adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- Usage policies require explicit consent from authorized parties to use the technologies.
- Usage policies require all technology use be authenticated with user ID and password or other authentication item (for example, token).
- Usage policies require a list of all devices and personnel authorized to use the devices.
- Usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.
- Usage policies require acceptable uses for the technology.
- Usage policies require acceptable network locations for the technology.
- Usage policies require a list of company-approved products.
- Usage policies require automatic disconnect of sessions for remote access technologies after a specific period of inactivity.
- Usage policies require activation of remote access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.
- Usage policies prohibit copying, moving or storage of cardholder data onto local hard drives and removable electronic media when accessing such data via remote access technologies.

12.3 PROCEDURE

Department of Technology Services (DTS) has developed and implemented comprehensive Usage policies for critical employee-facing technologies, which encompass the following categories and supporting activities. These policy directives and supporting procedures will be fully enforced by *Department of Technology Services (DTS)* for ensuring the Usage policies for critical employee-facing technologies are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by *Surplus Property*.

EXPLICIT MANAGEMENT APPROVAL TO USE THE TECHNOLOGIES

Due to the abundance of technologies afforded by today's technology environment, *Department of Technology Services (DTS)* requires explicit management approval for the use of these technologies in conjunction with one's professional roles and responsibilities. The phrase, *explicit management approval*, consists of the following approval mechanisms and initiatives for the technologies listed below, along with an explicit Usage policy for each respective technology:

Technologies	Management Approval Process	Usage Policy
Network Devices	All system administrative users of network devices (Firewalls, Routers, Switchgear, Load Balancers, Intrusion Detection Systems) and other related network devices must gain management approval via the following formalized and documented process:	(1) All network devices are to be configured and used strictly for business operations. (2) All network devices are to be appropriately hardened and secured in accordance with industry standards and for applicable business requirements. (3) Network components may not be added, removed or modified unless explicit consent is granted by appropriate personnel. (4) Any network devices obtained without proof of purchase and licensing rights will not be allowed onto the network. (5) All users (system administrative users) must be responsible for the proper use of these devices. (6) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these devices will not be tolerated. (7) All network system administrative rights and subsequent activities are subject to audit and review as needed. (8) Violation of these usage policies is grounds

		for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy

Operating Systems	All system administrative users and end-users of operating systems (Windows, UNIX, LINUX) and other related operating systems must gain management approval to use these systems devices via the following formalized and documented process	(1) All operating systems are to be configured and used strictly for business operations. (2) All operating systems are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Operating systems may not be added, removed or modified unless explicit consent is given by appropriate personnel. (4) Any operating system obtained without proof of purchase and licensing rights will not be allowed onto the network. (5) All users (system administrative users) must be responsible for the proper use of these operating systems. (6) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these operating systems will not be tolerated. (7) All system administrative rights and subsequent activities are subject to audit and reviews as needed. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Applications	All users of applications (coders/developers, end-users of applications, etc.) must gain management approval to use these applications via the following formalized and documented process	(1) All applications (internally developed and commercially purchased) are to be configured and used strictly for business operations. (2) All applications are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Applications may not be added, removed or modified unless explicit consent is given by appropriate personnel. (4) Any application obtained without proof of purchase and licensing rights will not be allowed onto the network. (5) All users (coders/developers, end-users) must be responsible for the proper use of these applications. (6) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these applications will not be tolerated. (7) All users and their respective functions for any applications are subject to audit and reviews as needed. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Databases	All users of databases (database administrators, end-users of databases, etc.) must gain management approval to use these databases via the following formalized and documented process:	(1) All databases are to be configured and used strictly for business operations. (2) All databases are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Databases (and their representative elements, such as database files) may not be added, removed or modified unless explicit consent is given by appropriate personnel. (4) Any databases obtained without proof of purchase and licensing rights will not be allowed onto the network. (5) All users (database administrators, end-users of databases, etc.) must be responsible for the proper use of these technologies. (6) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these technologies will not be tolerated. (7) All database system administrative rights and subsequent activities are subject to audit and reviews as needed. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Remote Access Technologies	All end-users of remote access technologies (VPN, Remote Desktop Protocols, etc.) must gain access to use these remote access technologies via the following formalized and documented process:	(1) All remote access technologies are to be configured and used strictly for business operations. (2) All remote access technologies are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Remote access technologies may not be added, removed or modified unless explicit consent is given by appropriate personnel. (4) Any remote access technologies and their supporting protocols obtained without proof of purchase and licensing rights will not be allowed onto the network. (5) All end-users must be responsible for the proper use of these technologies. (6) Automatic disconnect of sessions for remote access technologies after a specific period of inactivity is required. (7) Activation of remote access technologies used by vendors occurs only when needed by vendors and with immediate deactivation after use. (8) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these remote access technologies will not be tolerated. (9) All end users and subsequent activities are subject to audit and reviews as needed. (10) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Wireless Technologies	All end users of wireless technologies (Wi-Fi/hotspots) must gain access to use these wireless technologies via the following formalized and documented process:	(1) All wireless technologies are to be configured and used strictly for business operations. (2) All wireless technologies are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Wireless technologies may not be added, removed or modified unless explicit consent is given by appropriate personnel. (4) Any wireless technologies obtained without proof of purchase and licensing rights will not be allowed onto the network. (5) All end-users must be responsible for the proper use of these technologies. (6) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these wireless technologies will not be tolerated. (7) All end users and their subsequent activities are subject to audit and reviews as needed. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Removable Electronic Media	All users of removable electronic media (external hard drives, USB drives, memory sticks, etc.) must gain access to use these devices via the following formalized and documented process:	(1) All removable electronic media devices are to be configured and used strictly for business operations. (2) All removable electronic media devices are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) All users must be responsible for the proper use of these technologies. (4) Users are prohibited from copying, moving or storage of cardholder data onto local hard drives and removable electronic media when accessing such data via remote access technologies (5) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these removable electronic media devices will not be tolerated. (6) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Desktops	All users of desktops must gain access to use these computers via the following formalized and documented process	(1) All desktops are to be configured and used strictly for business operations. (2) All desktops are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Desktops may not be added, removed or modified unless explicit consent is given by appropriate personnel. (4) Any desktop obtained without proof of purchase and licensing rights will not be allowed onto the network. (5) All end-users must be responsible for the proper use of these technologies. (6) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of desktops will not be tolerated. (7) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Laptops	All users of laptops must gain access to use these computers via the following formalized and documented process:	(1) All laptops are to be configured and used strictly for business operations. (2) All laptops are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Any laptop obtained without proof of purchase and licensing rights will not be allowed onto the network. (4) All end-users must be responsible for the proper use of these technologies. (5) Users must protect their company-issued laptop from loss, theft and damage, and must also report loss or theft to designated personnel in a timely manner. (6) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of laptops will not be tolerated. (7) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Personal Data Assistants	All users of company issued PDAs must gain access to use these devices via the following formalized and documented process:	(1) All PDA devices are to be configured and used strictly for business operations. (2) All PDA devices are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3). Any PDA device obtained without proof of purchase and licensing rights will not be allowed onto the network. (4) All users must be responsible for the proper use of these technologies. (5) Users must protect their company-issued PDA device from loss, theft and damage, and must also report loss or theft to designated personnel in a timely manner. (6) Only non-confidential information may be stored on a PDA device, as it is not considered a secure device. (7) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of PDA devices will not be tolerated. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Cell Phone	All users of company-issued cell phones must gain access to use these devices via the following formalized and documented process:	(1) All cell phones are to be configured and used strictly for business operations. (2) All cell phones are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. (3) Any cell phone obtained without proof of purchase and licensing rights will not be allowed onto the network. (4) All users must be responsible for the proper use of these technologies. (5) Users must protect their company-issued cell phone from loss, theft and damage, and must also report loss or theft to designated personnel in a timely manner (6) Only non-confidential information may be stored on a cell phone, as it is not considered a secure device. (7) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of cell phones will not be tolerated. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Internet Use	All users of the internet must gain access to use this technology via the following formalized and documented process:	(1) All users are responsible for their internet activity and are encouraged to use the internet in a judicious and ethical manner at all times. (2) The internet is to be used for business purposes, but may be used for personal necessities from time to time. (3) Connections to the internet are to be conducted through company-approved technologies and resources only. (4) No insecure ports, protocols or services are to be used on the internet by any user. (5) Users are not allowed to visit any pornographic sites or download any offensive material including, but not limited to pornography and other material deemed offensive in nature. (6) Users may not use the internet to facilitate personal financial gain while at work. (7) Users may not use the internet to incite violence or conduct any other activity deemed criminal or offensive in nature. (8) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of the internet will not be tolerated. (9) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Email Use	All users of email must gain access to use this technology via the following formalized and documented process:	(1) All users are responsible for their email activity and are encouraged to use email in a judicious and ethical manner at all times. (2) Email is to be used for business purposes, but may be used for personal necessities from time to time. (3) Connections to the internet for the use of email are to be conducted through company-approved technologies and resources only. (4) No insecure ports, protocols or services are to be used for email activities. (5) Users are not allowed to send or receive offensive material via email including, but not limited to pornography and other material deemed offensive in nature. (6) Users may not use email to facilitate personal financial gain while at work. (7) Users may not use email to incite violence or conduct any other activity deemed criminal or offensive in nature. (8) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of email will not be tolerated. (9) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Blogging	All user who blog on various internet forums must gain access to blog via the following formalized and documented process:	(1) All users are responsible for their blogging activity and are encouraged to blog in a judicious and ethical manner at all times. (2) Blogging is to be used for business purposes, and only on approved sites. (3) Users are not allowed to blog about offensive material including, but not limited to pornography and other material deemed offensive in nature. (4) Users may not use blogging to facilitate personal financial gain while at work. (5) Users may not use blogging to incite violence or conduct any other activity deemed criminal or offensive in nature. (6) Users are not permitted to blog about any confidential information pertaining to the organization. (7) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of blogging will not be tolerated. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

Technologies	Management Approval Process	Usage Policy
Social Media Forums	All users who interact and participate on social media forums must gain access to these forums via the following formalized and documented process:	(1) All users are responsible for their social media activity and are encouraged to blog in a judicious and ethical manner at all times. (2) Social media is to be used for business purposes, and only on approved sites. (3) Users are not allowed to use social media as a forum for promoting offensive material including, but not limited to pornography and other material deemed offensive in nature. (4) Users may not use social media to facilitate personal financial gain while at work. (5) Users may not use social media to incite violence or conduct any other activity deemed criminal or offensive in nature. (6) Users are not permitted to use social media as a forum for discussing any confidential information pertaining to the organization. (7) Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of social media will not be tolerated. (8) Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

USE OF ALL TECHNOLOGY RESOURCES MUST BE AUTHENTICATED

Accessing system components and any other IT resources deemed critical by the organization requires the use of a user ID and a password.

The following password parameters are to be enforced and used when accessing technologies such as network devices, operating systems, applications or databases (Security Standards Council, Version 3.2):

- User password parameters are set to require users to change passwords at least every ninety (90) days.
- Password parameters are set to require passwords to be at least seven (7) characters long.
- Password parameters are set to require passwords to contain both numeric and alphabetic characters.
- Password parameters are set to require that new passwords cannot be the same as the previous four (4) passwords.
- Password parameters are set to require that a user's account is locked out upon the sixth (6^{th}) invalid logon attempt.
- Password parameters are set to require that once a user account is locked out, it remains locked for a minimum of thirty (30) minutes or until a system administrator resets the account.
- System/session idle time out features have been set to fifteen (15) minutes or less.

LISTING AND LABELING OF ALL DEVICES AND PERSONNEL AUTHORIZED TO USE THEM

The following devices have been assigned to *Surplus Property* employees for business use. Due care is to be exercised in protecting the devices and all confidential company information contained in them. This list is to be updated to ensure that all records are kept current.

Owner/User of Device	Device	Contact Information	Purpose of Use

ACCEPTABLE USE

Surplus Property's technology resources provide users the ability to communicate for personal and professional reasons. These resources and the ability to use them are considered a privilege, and as such, users are expected to act responsibly and professionally at all times. Users utilizing *Surplus Property*'s technology resources must respect the rights of other users, the integrity of the systems and related physical resources, and they must obey all applicable laws and regulations (local, state and federal). Technology resources have vast capabilities of sending, receiving and storing electronic data; therefore, users must be particularly careful to protect these

technology resources and the associated data, and they must strictly adhere to software licensing agreements and copyright laws.

GENERAL GUIDELINES, RESPONSIBILITIES AND ACCEPTABLE USE FOR THE TECHNOLOGY

- The primary purpose and use of technology resources is for *Surplus Property* business activities only.
- Users do not own any accounts; rather, they are granted access commensurate with their roles and responsibilities within the organization.
- Users are never to share their accounts with others and must keep all password information confidential.
- It is the responsibility of any user given access rights to the account to protect its access.
- Users must strictly adhere to licensing agreements and copyright laws that govern all material accessed or stored using *Surplus Property*'s technology resources.
- Users are not permitted to develop or use programs that affect other users.
- Users are not permitted to develop or use programs that may cause harm to the organization's computer systems.
- Users are not permitted to use any type of services that result in restricting network access from other users.
- Users are not permitted to use any type of services that significantly impair access to other networks connected to *Surplus Property*.
- Users remotely accessing *Surplus Property]*'s systems are responsible for using protocols for remote access approved by *Department of Technology Services (DTS)*.
- Users shall not intentionally seek information on, or represent themselves as, another user unless permitted to do so by that user or by authorized personnel.
- Users are not permitted to obtain information belonging to other users. This includes but is not limited to the following: passwords, data files and other sensitive and confidential information.

UNACCEPTABLE USE AND BEHAVIOR

- Using or attempting to use another user's account to access resources
- Using or attempting to use *Surplus Property*'s technology resources to gain unauthorized access to company-wide systems
- Using or attempting to use *Surplus Property*'s technology resources for purposes of sexual harassment, threats against the organization or any other type of civil or criminal misconduct
- Violating any copyright laws by obtaining any form of media or resources using *Surplus Property*'s technology resources

- Spamming or mass solicitation of company material to known or unknown third parties
- Releasing prohibited and classified company information to the public through the use of *Surplus Property*'s technology resources
- Intentionally installing any unapproved equipment to the *Surplus Property* infrastructure

DISCIPLINARY ACTION

Any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of social media will not be tolerated. Violation of these Usage policies is grounds for being reprimanded, suspended or terminated.

ACCEPTABLE NETWORK LOCATIONS FOR THE TECHNOLOGY

All *Surplus Property]*'s technology resources are to be appropriately configured, hardened and physically and logically placed within the network so as not to create any inherent security weaknesses for the respective system or any other supporting systems. Please refer to network diagram for a complete listing of the physical and logical placement of all technology resources.

LIST OF COMPANY-APPROVED PRODUCTS

State of Utah is the legal owner of all technology resources purchased or leased with company funds. The overall responsibility for administering and overseeing these technology resources rests with *Department of Technology Services (DTS)*. Provided below is a list of *Department of Technology Services (DTS)*-approved technologies that may be used within the business environment of the organization.

Technologies	List of Approved Products	Name and Title of Approver
Network Devices	*See DTS purchasing policies and architectural board for DTS*	
Operating Systems	" "	
Applications	" "	
Databases	" "	
Remote Access Technologies	" "	
Wireless	" "	

Technologies		
Removable Electronic Media	" "	
Desktops	" "	
Laptops	" "	
Personal Data Assistants (Company-provided)	" "	
Cell Phone (Company-provided)	" "	
Internet Use	" "	
Email use	" "	
Blogging	" "	
Social Media Forums (Company-sponsored Sites)	" "	

ADDITIONAL USAGE POLICY REQUIREMENTS (Security Standards Council, 2010)

- Automatic disconnect of sessions for remote access technologies after a specific period of inactivity
- Activation of remote access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use
- Prohibiting the copying, moving or storage of cardholder data onto local hard drives and removable electronic media when accessing such data via remote access technologies

12.3 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Department of Technology Services (DTS)* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

** Comply with Utah Administrative Code R895 required, (http://rules.utah.gov/publicat/code/r895/r895.htm), & DTS State wide Policies (https://dts.utah.gov/policies)

REQUIREMENT 12.4 TO 12.5.5

INFORMATION SECURITY RESPONSIBILITIES

12.4 TO 12.5.5 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Department of Technology Services (DTS)* has established a formal policy and supporting procedures concerning information security responsibilities. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

12.4 TO 12.5.5 POLICY

Department of Technology Services (DTS) will ensure that the Information Security Responsibilities policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council, Version 3.2):

- Information Security policies clearly define information security responsibilities for both employees and contractors and all other personnel.
- Formal assignment of information security is to be given to a Chief Security Officer or other security-knowledgeable member of management.
- The responsibility for creating and distributing security policies and procedures is to be formally assigned to authorized personnel.
- The responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is to be formally assigned to authorized personnel.
- The responsibility for creating and distributing security incident response and escalation procedures is to be formally assigned to authorized personnel.

- The responsibility for administering user account and authentication management is to be formally assigned to authorized personnel.
- The responsibility for monitoring and controlling all access to data is to be formally assigned to authorized personnel.

12.4 TO 12.5.5 PROCEDURE

Department of Technology Services (DTS) has developed and implemented a comprehensive program regarding information security responsibilities, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *Department of Technology Services (DTS)* for ensuring that the information security responsibilities initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by D*epartment of Technology Services (DTS)*.

INFORMATION SECURITY RESPONSIBILITIES FOR EMPLOYEES AND CONTRACTORS

All employers and contractors utilizing and having access to a broad range of *Department of Technology Services (DTS)* information systems are required to adhere to the policies, procedures, provisions and general guidelines outlined in this security policy document and all other applicable supporting policy and procedure documents. Information security responsibilities include but are not limited to the following system components and any other IT resources deemed critical by *Department of Technology Services (DTS)*:

- Network devices and supporting network protocols and activities
- Operating systems and supporting systems
- Applications and supporting systems and activities
- Databases
- Data transmission protocols
- End-user devices and technologies

Information security responsibilities include not engaging in any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of system components or any other IT resources deemed critical by the organization. Violation of these information security responsibilities is grounds for being reprimanded, suspended or terminated.

FORMAL ASSIGNMENT OF INFORMATION SECURITY

The formal assignment of information security is to be given to and directed by a Chief Security Officer or other security-knowledgeable member of management. This individual will be

responsible for all facets of information security, which include but are not limited to the following:

- Oversight of all information security initiatives
- Approval of all Information Security policies, procedures, provisions and general guidelines
- The administration and assignment of information security activities to authorized personnel within the organization
- Ensuring that all information security initiatives are aligned with all company-wide regulatory compliance, governance and security mandates

Information Security Director	Title	Notes and Comments
Philip Bates	*CISO*	*In charge of all aspects of information security responsibilities, initiatives and mandates*

INFORMATION SECURITY RESPONSIBILITIES MATRIX

Responsibility	Responsibility Formally Assigned to the Following Personnel (Name and Title)	Contact Information (Email and Direct Dial Number)	Notes and Comments
Creating and distributing security policies and procedures	*DTS*		
Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel	*DTS Security*		

Creating and distributing security incident response and escalation procedures	*“ “*		
Administering user account and authentication management	*HR & DTS*		
Monitoring and controlling all access to data	*DTS - Agencies*		

12.4 TO 12.5.5 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Department of Technology Services (DTS)* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

REQUIREMENT 12.6

FORMAL SECURITY AWARENESS PROGRAM

12.6 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Department of Technology Services (DTS)* has established a formal policy and supporting procedures concerning a Formal Security Awareness program. This policy is to be implemented immediately. It will be evaluated on a(n) *annual* basis for ensuring its adequacy and relevancy regarding *Department of Technology Services (DTS)*'s needs and goals.

12.6 POLICY

Department of Technology Services (DTS) will ensure that the Formal Security Awareness program adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (NIST, n.d.):

- The Formal Security Awareness program, henceforth referred to as the *program*, consists of a scope and supporting material that are sufficient to meet the needs of *Department of Technology Services (DTS)* for security awareness initiatives.
- The phases of the program consist of the following:
    - Design
    - Develop
    - Implement
    - Maintain/Oversight
- The core tenants of the program consist of the following:
    - Awareness
    - Training
    - Education

12.6 PROCEDURE

Department of Technology Services (DTS) has developed and implemented a comprehensive program regarding formal security awareness, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *Department of Technology Services (DTS)* for ensuring the Security Awareness program initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources.

PROGRAM PHASES

In developing the program, *Department of Technology Services (DTS)* has adopted the core principles of *Design*, *Develop*, *Implement* and *Maintain/Oversight*, which assist in developing policies, processes, procedures, activities and supporting material that meet the security needs of our organization. These program phases are not static, as they are constantly evaluated and modified to ensure that *Department of Technology Services (DTS)* stays abreast of significant security issues threatening our organization and our clients, while simultaneously meeting the needs of all employees. The goal of the program is to have in place a comprehensive framework that successfully addresses the core components of any program, which are *Awareness, Training* and *Education*.

DESIGN

In designing the program, *Department of Technology Services (DTS)* sought to (NIST, n.d.)—

- Identify and structure organizational training needs and overall awareness

- Conduct a comprehensive assessment of needs
- Develop an Awareness Training plan and establish priorities
- Determine the level of complexity of the program and the associated supporting material
- Allocate program funds

IDENTIFY AND STRUCTURE ORGANIZATIONAL TRAINING NEEDS

A critical component of the program's success was determining the model or architecture in which all facets of the program's strategy were to be implemented. The following models were discussed and investigated by *Department of Technology Services (DTS)* in order to determine the most appropriate fit for our organization (NIST, n.d.):

- **CENTRALIZED MODEL:** This model adheres to the principle of a central authority having responsibility (both operationally and financially) of the entire program. This central authority coordinates all essential aspects of the program, giving any necessary guidance. Furthermore, this centralized program or authority was found to be conducive to smaller organizations having highly centralized structure and environment along with similar needs and goals throughout the enterprise. In summary, the policies, strategies and activities for implementation were centralized.

- **MODERATELY DECENTRALIZED MODEL:** This model was found to be similar to that of the Centralized Model, but differed in regards to its implementation. Delegation authority was given to additional personnel (such as management of functional divisions and departments) for various aspects of the program. This moderately decentralized program was found to be conducive to larger organizations having a more decentralized structure and environment. In summary, the policies and strategies were centralized with implementation being distributed.

- **ENTIRELY DECENTRALIZED MODEL:** This model allows for a centralized policy with strategy and implementation being distributed. Generally, management such as a CIO or CTO is responsible for broad-based policy, but the strategy and implementation of the program is delegated to additional personnel (such as managers, as defined by the organization). In summary, the policies were centralized with strategies and implementation being distributed.

After extensive conferring amongst management, *Department of Technology Services (DTS)* chose to adhere to the **DECENTRALIZED MODEL**

COMPREHENSIVE ASSESSMENT OF NEEDS

In determining the needs of the program, *Surplus Property* sought to identify all key personnel within the organization and obtain their input regarding their requirements for the program. Specifically, the following personnel were involved in assessing the needs of the program for their respective divisions, departments and organizations within *State of Utah*.

- Senior management
- Facility and security personnel (physical and environmental security)
- Operational personnel
- Information technology/information systems personnel
- Administrative personnel
- Sales and marketing personnel

As a result of this process, the following personnel were involved in assessing the needs of the program for *Surplus Property*: (DTS Policy, Time King - Network, Akemi Dean - Applications, Bart Grant - Logs)

Senior Management	Facility and Security Personnel	Operational Personnel	Information Technology/Information Systems Personnel	Administrative Personnel	Sales and Marketing Personnel

DEVELOP TRAINING STRATEGY PLAN

A core component of the program's success was developing a Training Strategy plan that covered a number of important issues for ultimately ensuring the success of the overall program. Surplus Property/DTS discussed and examined the following subject matter in regards to the Training Strategy plan:

- **Program scope:** Which specific topics and material would comprise the program?

- **Roles and responsibilities within the program:** Included all phases of the program, from beginning (design) to end (maintain/oversight), along with any additional phases as needed
- **Goals of the program:** Which specific goals and associated deliverables were to be achieved as a result of the program?
- **Audience:** Which personnel within the organization would be exposed to the program and would become part of a *required* or *mandatory* audience?
- **Documentation and duration:** Which documents (hardcopy) and available resources (online) would comprise the program, and how often would the program be exposed to the required or mandatory audience?
- **Complexity and detail:** How in-depth and complex should the program be, and what specific subject matter should be discussed in accordance with the various departments, divisions and personnel within the organization?

As a result of these discussions Surplus Property/DTS developed a comprehensive program which effectively addressed these issues. The details of these initiatives are illustrated in subsequent sections within the document throughout the *Develop*, *Implement* and *Maintain/Oversight* sections.

DEVELOP

In developing the program, Surplus Property/DTS sought to—

- Develop material to be used for security awareness
- Identify and select relevant and critical topics to discuss
- Identify source material to be used for awareness
- Refine material and develop a model for training employees on security awareness

DEVELOP MATERIAL AND SELECT RELEVANT TOPICS

Surplus Property/DTS engaged in a comprehensive process for determining which specific training material the program would consist of and the relevant topics to include. As a result of this process, Surplus Property/DTS identified the following material and relevant topics to be included in the program:

- Senior management roles and responsibilities within the organization
- Facility and security personnel (physical and environmental security) roles and responsibilities within the organization
- Operational personnel roles and responsibilities within the organization

- Information technology/information systems personnel roles and responsibilities within the organization
- Administrative personnel roles and responsibilities within the organization
- Sales and marketing personnel roles and responsibilities within the organization
- Change management functions
- Incident response
- Customer service functions
- System access, including provisioning and deprovisioning activities, password complexity rules and requirements and remote access and system administrative rights
- Network access and monitoring, such as network user, network administrative rights, network monitoring, logging and reporting, anti-virus, patch management network maintenance and the protection of the network (DDOS, DOS, worms, malicious code, unknown email and attachments)
- Media backup, transport and logging activities
- Policy and procedures, such as their relevancy, accuracy, updating and monitoring and acknowledging them
- Software licensing issues
- Social engineering
- Portable memory devices, such as external hard drives, USB and other memory devices
- Wireless, such as which security precautions are in place for wireless
- Encryption of sensitive card holder data for the cardholder data environment
- Internet usage
- Inventory measures in place for all State-owned property
- Daily operational procedures outside of the above listed items

[Please add additional topics that your organization feels would be essential to any Formal Security Awareness program, and delete any of the above listed items if you feel they do not fall into the scope of your organization. The list above is considered comprehensive, and most organizations, at a baseline minimum, should address all the mentioned issues. Please note that all topics you list here will be added to a formalized matrix in a subsequent section.]

IDENTIFY SOURCE MATERIAL TO BE USED

Department of Technology Services (DTS) engaged in a comprehensive process for determining which source materials to use for the program. As a result of this process, *Department of Technology Services (DTS)* identified the following source material to be included in the program (NIST, n.d.):

- Professional vendors specializing in security awareness training
- Technology forums and user groups

- Periodicals and industry-specific publications
- Material obtained from seminars, trade shows and other events

[These are essentially the sources you will use to include in your Formal Security Awareness program. A common search for security awareness training *on the internet will provide you with numerous links to companies that specialize in this. These companies can provide remote training or send you material to use as part of your program, etc. Once you have identified which source material you will use, please list it below accordingly.]*

Professional Vendors Specializing in Security Awareness Training	Technology Forums and User Groups	Periodicals and Industry-specific Publications	Material Obtained from Seminars, Trade Shows and Other Events	Other
DTS Training	" "	" "	" "	" "

REFINE MATERIAL AND DEVELOP MODEL FOR TRAINING EMPLOYEES

After identifying the relevant topics, subject matter, sources and material to be used for the program, *Department of Technology Services (DTS)* began a comprehensive process of refining the material and developing a structure for the program. The following models are to be used for the program:

- Program model derived from topics, subject matter, sources and material obtained by third-party external vendors
- Program model derived from topics, subject matter, sources and material obtained by internal personnel
- Program model derived from topics, subject matter, sources and material derived from a mixture of external vendors and internal personnel

[Please discuss the content of the program (which topics and subject matter it covers), discuss the source material used and from where it was obtained and, finally, which of the above three listed models is the program to which you adhere.]

Content of the Program (Topics and Subject Matter)	Source Material Used	Obtained from
Senior Management Roles and Responsibilities	?	?

Facility and Security Personnel (Physical and Environmental Security)	?	?
Operational Personnel Roles and Responsibilities	?	?
Information Technology/Information Systems Personnel Roles and Responsibilities	?	?
Administrative Personnel Roles and Responsibilities	?	?
Sales and Marketing Personnel Roles and Responsibilities	?	?
Change Management Functions	?	?
Incident Response	?	?
Customer Service Functions	?	?
System Access, including provisioning and de-provisioning activities, password complexity rules and requirements, remote access rights, system administrative rights	?	?
Network Access and Monitoring, such as network user and network administrative rights, network monitoring, logging and reporting, anti-virus, patch management network maintenance and the protection of the network (DDOS, DOS, worms, malicious	?	?

code, unknown email and attachments)		
Media Backup, Transport and Logging Activities	?	?
Policy and Procedures, such as their Relevancy, Accuracy, Updating, Monitoring and Acknowledgement thereof	?	?
Software Licensing Issues	?	?
Social Engineering	?	?
Portable Memory Devices, such as external hard drives, USB and other memory devices	?	?
Wireless, such as which security precautions are in place for wireless	?	?
Encryption of sensitive card holder data for the cardholder data environment	?	?
Internet Usage	?	?
Inventory measures in place for all State-owned property	?	?
Daily operational procedures outside of the above listed items	?	?

IMPLEMENT

In implementing the program, *Department of Technology Services (DTS)* sought to—

- Communicate and deliver the security awareness initiatives and training material throughout the organization to all employees.

COMMUNICATE THE PLAN TO ALL EMPLOYEES

After identifying the relevant topics, subject matter, sources, material and model to be used for the program, *Department of Technology Services (DTS)* began a comprehensive process of determining the best channels and modes for communicating and delivering critical aspects of the program (awareness and training) to employees. As a result of this process, *Department of Technology Services (DTS)* identified the following channels and modes for communicating and delivering awareness and training to employees:

COMMUNICATING SECURITY AWARENESS TO EMPLOYEES (NIST, n.d.)

- Posters, slicks and periodicals
- Special awareness meetings
- Email messages
- Web and/or videotape sessions

*[The above four (4) listed items are generally the best way to deliver ongoing security awareness issues that are considered relevant and critical to the organization. Please discuss how you will continually deliver these awareness issues to employees. Do not confuse this with the subsequent topic (*Delivering Training*), which illustrates how employees will actually take part in quarterly, semi-annual or annual training, which are formalized sessions.]*

DELIVERING TRAINING TO EMPLOYEES (NIST, n.d.)

- Video training
- Instructor-lead training
- Web-based training

[The above three (3) listed items are generally the best way to deliver actual training. Please discuss how this will actually be conducted for your organization.]

MAINTAIN/OVERSIGHT

In maintaining and overseeing the program, *[company name]* sought to—

- Effectively monitor adherence to the program
- Collect vital feedback as to the program's adequacy
- Effectively manage necessary changes to the program for improving the overall program itself

MONITOR ADHERENCE TO THE PROGRAM

Adherence to the program will consist of all employees acknowledging via signature on the Formal Security Awareness Program Acknowledgement form that they have taken part in the program, understand its content and will abide by the provisions it has set forth.

COLLECT VITAL FEEDBACK ON THE PROGRAM

Employees can provide feedback concerning the adequacy of the program via the Formal Security Awareness Program Acknowledgement form.

MANAGE CHANGES AS NEEDED FOR THE PROGRAM

Changes to the program will be made as necessary to ensure that it meets the requirements for all employees. All changes will be approved by authorized personnel. Listed below is a list of changes that have been made to the program:

Section of Program to which changes were made (this includes all phases): (1)Design (2)Develop (3)Implement (4)Maintain/Oversight	Changes Made	Reason for Changes	Date of Changes
?	*?*	*?*	*?*

CORE COMPONENTS

By adhering to the three (3) main principles of Awareness, Training and Education, *Department of Technology Services (DTS)]* successfully met the intent and rigor of the program.

12.6 RESPONSIBILITY FOR POLICY MAINTENANCE

The *Department of Technology Services (DTS)* is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

- **Comprehensive PowerPoint slide presentation.** To be used for training all employees on PCI DSS specific security awareness initiatives.
- **In-depth security awareness training manual.** Complete with a signature acknowledgement form - to be given to each employee as a quick reference guide on important security issues.
- **Security Awareness Secure Coding Training Checklist.** A must-have document for any organization developing or offering web-based software products and services.
- **Employee Tracking Sheet.** Excel template for effectively tracking all employee security awareness training initiatives, such as start date, completion, and more.
- **Certificate of Completion template. T**o be awarded to each employee upon successfully viewing the PowerPoint slide presentation and reading the security awareness training manual.

REQUIREMENT 12.10.1

INCIDENT RESPONSE PLAN IN THE EVENT OF SYSTEM BREACH POLICY AND PROCEDURES

12.10.1 OVERVIEW

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *Surplus Property* has established a formal policy and supporting procedures for the incident response plan to be implemented in the event of a system breach. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding *Surplus Property*'s needs and goals.

12.10.1 POLICY

Surplus Property will ensure that an incident response plan in the event of system breach adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.2):

- Report to Department of Technology Services (DTS)
- Report to Department of Finance PCI Compliance Coordinator
- Report to Surplus Property Manager

12.10.1 PROCEDURE

Surplus Property has developed and implemented a comprehensive program regarding incident response plan in the event of system breach and supporting activities listed below. These policy directives will be fully enforced by *Surplus Property* for ensuring that the incident response plan in

the event of system breach is executed in a formal manner. Reporting will be done immediately both by phone or online to DTS (Reference ICN #) and by phone and email to PCI Compliance Coordinator and Surplus Property Manager. (The ICN# will be provided to each) The table below is contact information for reporting;

SYSTEM BREACH REPORTING INFORMATION

Name	Title	Contact Information	Website/Email	Reference
DTS	*Desktop Support*	*801-538-3440*	*dts.utah.gov*	*DTS Ticket (ICN #)*
Finance	*PCI Compliance Coordinator*	*Cory Weeks 801-538-3173*	*cweeks@utah.gov*	*Email*
Surplus Property	*Manger*	*Dan Martinez 801-619-7219*	*danmartinez@utah.gov*	*Email*

12.10.1 RESPONSIBILITY FOR POLICY MAINTENANCE

Surplus Property is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.