VIRTUALIZATION

General Overview

Virtualization, in the context of information systems, is essentially the virtualizing of physical systems into "virtual" elements, such as computer platforms, operating systems (OS), storage devices, or computer network resources, and more. It's a concepts that's firmly taken root, with organizations all throughout the globe adopting virtualization platforms. Yet it's equally important that numerous information security best practices be put in place for ensuring the confidentiality, integrity, and availability (CIA) of virtualized platforms. Though virtualization is a massive and growing field, for purposes of the below referenced policies and procedures, the concept of "hardware" and "full" virtualization is in scope for such documentation, hence phrases such as "hypervisors", "virtual machine monitors", "guest O/S", etc. will be covered. As for the main virtualized platforms being used by companies, they generally consist of the following:

- VMware
- Citrix XenServer
- Microsoft Hyper-V
- Red Hat Enterprise Virtualization

Though virtualization has without question brought about greater speed, efficiencies, and long-term cost savings, great benefits also come with great risks. One of the biggest challenges of virtualization is that of all computing resources being condensed onto one physical computing resource, which can be catastrophic if hardware issues are encountered, from failing disks to physical damage, etc. Additionally, sharing of resources, information, and other data on virtualized environments also means that malware and other malicious threats can spread just as easily, conceivably infecting an entire virtualized platform. Comprehensive security measures for virtualized platforms begin by implementing in-depth, well-written policies and procedures covering all essential topics, from provisioning and hardening, change management, patching, just to name a select few initiatives. The below referenced material should be looked upon as industry leading security documentation for helping ensure the confidentiality, integrity, and availability (CIA) of virtualization platforms.

Key terms and definitions within the scope of this documentation includes the following:

Virtualization: Virtualization is the process of partitioning physical computing resources into logical elements, thus resulting in logically isolated, stand-alone instances, such as servers, and their underlying operating systems and applications.

Hypervisor: A hypervisor (also called virtual machine monitor or virtual machine manager) is critically important, as it serves as the program residing on the actual "bare metal" hardware of the physical machine, effectively allowing multiple computing resources (i.e., operating systems) to run on the machine (i.e., host computer). This in turn allows guest machines (i.e., virtual machines) to "think" they have their own resources, ultimately allowing for virtualization to work.

Virtual Machine: As for the virtual machine, which is often called a “guest O/S” or “instance”, it’s a self-contained computing resource with its own operating system, and other necessary resources. It functions independently - logically speaking - from the virtual machine monitor, yet requires its underlying resources to work.

Citrix XenServer Virtualization Policy and Procedures

Title	**[company name] Citrix XenServer Virtualization Policy and Procedures**
Version	Version 1.0
Date	TBD
Language	English
Individual and/or Department Responsible for Distribution of Document	[company name] Information Technology Department
Individual and/ or Department Responsible for Timely Update of Document	[name and title]
Developed by:	[company name]
Subject	Database
Approval Date	TBD
Purpose of Document	To implement comprehensive Citrix XenServer virtualization policies, procedures, and practices whereby all employees and other intended parties are readily aware of the organization's Citrix XenServer virtualization uses and rights.
Distribution of Document	Disbursed to all employees of [company name] and available by request to all other intended parties.

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Citrix XenServer virtualization policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Citrix XenServer virtualization policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of the organization's virtualization platforms and all interconnecting systems and devices.

1.0 Scope

This policy and supporting procedures encompasses all Citrix XenServer systems that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of Citrix XenServer systems.

- Please note that when referencing the term "Citrix XenServer systems", "system resource(s)", or any variant thereof, this pertains to the following four (4) core components: (1). The actual server itself and the underlying hardware (i.e., physical, stand-alone server or virtual server): (2). The underlying operating system (OS) residing on the server, specifically, the host O/S. (4). Guest Operating Systems (O/S), guest instances, etc. (3). Any additional software (i.e., vendor specific, open source, internally developed applications, etc.) residing on the server. Thus, the below referenced policies and supporting procedures have been designed to effectively address various operational, technical, and security measures for both the OS and all software residing on the server itself.

1.0 Policy

[Company name] is to ensure that the Citrix XenServer virtualization policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Data and Information Classification

Data and information being stored, processed, and/or transmitted on system resources that are owned, operated, maintained and controlled by [company name] are to have appropriate classification levels in place that consist of the following:

- Unclassified | Public Information: This type of data and information, and the underlying information assets associated with it, is generally designed to be used by anonymous individuals or systems that have a credible interest in communicating with [company name]. As such, this type of data and information is disclosed freely to the general public.
- Proprietary: This type of data and information, and the underlying information assets associated with it, is generally designed to be used by internal employees only, thus it's prohibited from being circulated outside of the organization.
- Confidential: This type of data and information, and the underlying information assets associated with it, is intended to be viewed and/or utilized by select employees only.
- Company Confidential: This type of data and information must be protected from unauthorized access at all times, but with a focus on the data and information being that of internal, corporate issues.
- Client Confidential: This type of data and information must be protected from unauthorized access at all times, but with a focus on the data and information being that of the customers.
- Sensitive: This type of data and information, and the underlying information assets associated with it, is intended to be viewed and/or utilized by very select employees only. Furthermore, it requires an extremely high level of protection from unauthorized parties for ensuring its confidentiality, integrity, and availability (CIA).
- Trade Secret: This type of data and information, and the underlying information assets associated with it, is also intended to be viewed and/or utilized by very select employees only. Furthermore, it too requires an extremely high level of protection from unauthorized parties for ensuring its confidentiality, integrity, and availability (CIA).
- Top Secret: This type of data and information, and the underlying information assets associated with it, is intended to be viewed and/or utilized by an extremely select number of employees only. Furthermore, it requires the highest levels of protection from unauthorized parties for ensuring its confidentiality, integrity, and availability (CIA).

An appropriate data and information classification level is to be identified and assigned for the specified system resource and documented accordingly during the initial provisioning steps as outlined in the Citrix XenServer Virtualization Provisioning and Hardening Checklist. **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package).**

Additionally, effective data and information management measures also require [company name] to define the following:

- Access rights
- Usage rights (i.e., copying, printing, sending, storing, an sharing)
- Physical Security
- Environmental Security
- Network Security

- Secure Transmission
- Backups
- Disposal and Sanitization
- Security Categorization

As such, each of the aforementioned data and information classification levels described within this section also contain detailed information regarding the above listed measures, for which interested parties can learn more about by accessing [company name]'s enterprise-wide Data and Information Classification policy and procedures document.

Security Categorization
All system resources owned, operated, maintained and controlled by [company name] are to have in place effective measures for ensuring their confidentiality, integrity, and availability (CIA). Specifically, "Confidentiality" in that information is protected from access and disclosure to unauthorized parties. "Integrity" in that information is authentic, has not been altered (i.e. modified, destroyed, deleted, removed, etc.) and cannot be modified undetectably. And "Availability" in that information is available to all authorized parties in a timely and consistent manner.

As such, all Citrix XenServer systems are to be hardened accordingly for ensuring the objectives of CIA are maintained at all times, while also being assigned a security category in accordance with the United States Federal Information Processing Standards Publication 199 (FIPS PUB 199), *"Standards for Security Categorization of Federal Information and Information Systems"*. This standard, which is officially issued by the National Institute of Standards and Technology (NIST), details the following three (3) security categories (i.e. "potential impact") that correspond to each one of the respective CIA objectives (confidentiality, integrity, and availability):

- Category | Impact: LOW-The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a LIMITED adverse effect on the organization.
- Category | Impact: MODERATE- The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a SERIOUS adverse effect on the organization.
- Category | Impact: HIGH- The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a SEVERE | CATASTROPHIC adverse effect on the organization.

The assigned security category, in accordance with FIPS PUB 199, as published by NIST, is to be identified and documented accordingly during the initial provisioning steps as outlined in the Citrix XenServer Virtualization Provisioning and Hardening Checklist. **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package).**

Physical Security
Appropriate security measures are to be implemented, which includes all necessary physical security controls, such as those related to the safety and security of the actual hardware (i.e., servers) for which the Citrix XenServer systems reside on. This requires the use of a computer room or other designated area (facility) that is secured and monitored at all times and whereby only authorized personnel have physical

access to the specified system resource. Thus, "secured" and "monitored" implies that the facility has in place the following physical security and environmental security controls:

- Constructed in a manner allowing for adequate protection of the Citrix XenServer systems.
- Security alarms that are active during non-business hours, with alarm notifications directly answered by a third-party security service or local police force.
- The use of cages, cabinets, or other designated, secured areas for securing the specified system resource.
- Access control mechanisms consisting of traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e. iris, palm, fingerprint scanners/readers). Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are retained for a minimum of [x] days.
- Adequate closed-circuit monitoring, video surveillance as needed, both internally and externally, with all video kept for a minimum of [x] days for purposes of meeting security best practices and various regulatory requirements.
- Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.
- Appropriate power protection devices for ensuring a continued, balanced load of power to the specified system resource, thus mitigating power surges and spikes.

Personnel

The phrases "authorized personnel" and "authorized individuals" are used throughout this policy and procedure document, and in doing so, [company name] mandates that employees responsible for general provisioning, maintenance and security of Citrix XenServer systems are those deemed to be professional, well-skilled, and competent individuals. Not only must they be capable of implementing procedures necessary for ensuring the confidentiality, integrity and availability (CIA) of the specified system resource, they must willingly continue to enhance their applicable skill-sets and subject matter knowledge relating to systems. Hardware and software solutions provided by vendors are only as good as the individual who deploy their services, thus [company name] I.T. employees are to strive at all times to continue to enhance their knowledge base with the following measures:

- Attending security and technology conferences and seminars, both online and at physical locations.
- Subscribing to alert forums, messaging boards and other online organizations and associations.
- Subscribing to hard-copy magazine and newsletter publications.
- Undertaking Continuing Professional Education (CPE) courses and related activities.
- Willingness to attain additional certifications within the Information Technology field as a whole.

Employees who undertake such measures are placing a high priority on the overall security and availability of [company name's] network, and in doing so, are promoting best practices for the organization, while also continuing to advance themselves professionally.

Security Awareness Training

All employees within [company name] are to undergo annual security awareness training initiatives for ensuring they stay abreast of significant security issues that pose a credible threat to the organization as a whole, including, but not limited to, [company name]’s network infrastructure and all supporting system

resources. While the goal of the program is to have in place a comprehensive framework that effectively addresses the core components of *Awareness, Training* and *Education*, the program must also provide subject matter directly related to the security of Citrix XenServer systems. Specifically, all users (both end-users and administrators) having access rights to Citrix XenServer systems must have adequate knowledge in understanding the threats associated to these specified system resources, along with the necessary response and resolution measures to undertake.

As such, the security awareness training program is to provide both general, enterprise wide training measures along with subject matter specifically related to Citrix XenServer systems. As previously stated, the program is to implement the core components of *Awareness, Training* and *Education*. "Awareness" in that numerous measures are initiated and implemented for keeping all employees knowledgeable about the threats, responses and solutions to security issues affecting [company name]. "Training" in that material is researched, developed and subsequently utilized for educating employees on all aspects of security awareness. And "Education" in that measures are undertaken for ensuring continuing education on security awareness is provided to all employees on a routine basis, rather than just a once-per year calendar activity. It must be stressed that security awareness training is dynamic in nature, changing as needed to meet the growing threats facing [company name].

Provisioning and Hardening

All systems, specifically the host O/S and other supporting hardware and software utilities, are to be properly provisioned, hardened, secured, and locked-down for ensuring their confidentiality, integrity, and availability (CIA). Improperly or poorly provisioned systems can often result in network exploitation by hackers, malicious individuals, and numerous other external, and internal threats. Therefore, the following provisioning and hardening procedures are to be applied as necessary when deploying Citrix XenServer systems onto [company name's] network:

- Vendor-supplied default settings are changed.
- All unnecessary accounts are eliminated.
- Only necessary and secure services, protocols and other essential services are enabled as needed for functionality.
- All unnecessary functionality is effectively removed.
- All system security parameters are appropriately configured.
- Documented system configuration standards are applied via a documented Citrix XenServer Virtualization Provisioning and Hardening checklist containing the following categories:

    - Operating System
    - System Auditing
    - System Access Controls
    - User Account Privilege Controls
    - Networking Security
    - Local Security Options

Provisioning and hardening all [company name] Citrix XenServer systems greatly increases its overall security in that insecure services that were effectively removed and/or disabled now cannot be used to attack and ultimately compromise the specified system resource. Additionally, the fewer the number of

services and protocols in use, the greater the chances of interoperability and compatibility with other system resources, both internally and externally. Furthermore, one's ability to comprehensively review and detect issues or concerns from Citrix XenServer systems log reports is much greater when only necessary services or protocols are enabled, rather than a myriad of settings that produces voluminous audit trails, which can be challenging to monitor.

Regarding provisioning and hardening, this critical and time-consuming process is to be undertaken by authorized personnel only; a select number of individuals who have the authority and applicable skill-sets to conduct these activities. Furthermore, strict adherence to the configuration settings stated within the documented Citrix XenServer Virtualization Provisioning and Hardening checklist is required at all times, with all necessary information (1. signature. 2 date. 3. any additional information, if necessary) completed by appropriate personnel.

Hypervisor Security Best Practices

Securing the Hypervisor and all associated programs and platforms that allow it to perform its functions are absolutely critical to the overall confidentiality, integrity, and availability (CIA) of Citrix XenServer systems. In accordance with numerous best practices, such as those offered by Citrix, NIST SP 800-125 publication, Guide to Security for Full Virtualization Technologies, and numerous other publications, the following security steps are to be undertaken:

- Thoroughly document (i.e., flowcharts, diagrams) the entire virtualization environment as necessary, and the supporting management architecture.
- Install all updates to the hypervisor as they are released by the vendor.
- Restrict administrative access to the management interfaces of the hypervisor itself.
- Utilize directory services for authentication.
- Place an important emphasis on root privileges, thus securing this type of account is of utmost importance.
- Limit access to powerful commands.
- Establish strong password policies for all accounts associated with the Hypervisor and all interconnecting systems.
- Limit software to those only necessary for the virtualization environment, which also included agents for audit trails and other regulatory compliance, security mandates.
- Establish and maintain file system integrity at all times.
- Put in place comprehensive logging and reporting capabilities.
- Strict access controls to the host O/S are to be in place to prevent someone from gaining access through the host O/S to the virtualization system and possibly changing its settings and/or even modifying the Guest O/Ss.
- Synchronize the virtualized infrastructure to a trusted authoritative time server, such as the NTP protocol.
- Disconnect any unused physical hardware from the host system.
- Disable all hypervisor services that can provide for possible attack vectors, such as file sharing, etc.
- Disable all unused services.
- Disable copy and paste functions between Guest O/S and remote console.

- Utilize in-depth capabilities for monitoring the security of each guest O/S.
- Vigilantly monitor the hypervisor itself for any signs of possible compromise, via the use of self-integrity monitoring capabilities that hypervisors may provide, as well as monitoring and analyzing hypervisor logs on a structured basis.
- Access to the virtualization management system should be restricted to authorized administrators only.
- Secure each hypervisor management interface, both locally and remotely accessible.
- If remote administration is enabled in a hypervisor, access to all remote administration interfaces should be restricted by a firewall, along with implementing security best practices for remote administration functions.
- Because the hypervisor provides unprecedented levels of access to and control over the guest O/S, limiting access to the hypervisor is critical to the security of the entire system.
- Document and define security policies about which guest O/S can be run from bare metal hypervisors and which can be run from hosted virtualization hypervisors.
- Provide physical access controls for the hardware on which the virtualization system runs.
- Minimize the number of applications other than the hypervisor that are ever run on the system.

Guest Machines | Guest O/S Security Best Practices

Securing the guest machines (i.e., Guest O/S, virtual instances, etc.) is also critically important in any virtualized environment, thus in accordance with numerous best practices, such as those offered by Citrix, NIST SP 800-125 publication, Guide to Security for Full Virtualization Technologies, and numerous other publications, the following security steps are to be undertaken:

- Follow all recommended best-practices for managing the actual physical O/S of the virtualized platform, as this ultimately helps ensure the safety and security of the Guest O/S.
- Install all updates to the guest O/S as required and in a prompt manner.
- Put in place comprehensive backup policies, procedures, and processes for the guest O/S, essentially using the same policy for backups as is used for non-virtualized computers in the organization.
- In each guest O/S, disconnect unused virtual hardware.
- Use separate authentication solutions for each guest O/S unless there is a compelling reason for multiple Guest O/S to share credentials.
- Ensure that virtual devices for the Guest O/S are associated only with the appropriate physical devices on the host system
- When possible, strive for building a hardened baseline Guest O/S, one with no applications, and use this for “spinning up” new virtual servers.
- Ensure appropriate controls, oversight, and safeguards are in place for provisioning and de-provisioning Guest O/S, and all related applications and their respective licenses.
- Apply network security best practices for logically isolating Guest O/S from one another.

Reference Material

Along with the stated policies, procedures, and supporting provisioning and hardening checklists provided within this document, additional reference material is widely available on the internet from a number of trusted sources. The following links and their applicable reference material have been

identified as those deemed credible in providing additional subject matter relating to general provisioning and hardening of Citrix XenServer systems.

- **http://support.citrix.com/**
  - Comprehensive support center provided by Citrix for many of their products and services, including XenServer, though they do not provide an actual hardening guide.

- Additionally, docstoc.com and slideshare.net, two well-known publishing portals, have a wealth of information relating to the installation, configuration, provisioning, and hardening for Citrix XenServer systems. These two (2) sites are great references for acquiring additional technical documentation on Citrix XenSeverver systems.

Time Synchronization

Correct, accurate and consistent time on all [company name] Citrix XenServer systems entails procedures for properly acquiring, distributing and storing time from industry accepted external sources; those which are based on Coordinated Universal Time (UTC), which is essentially based on International Atomic Time (TAI). And while there are several protocols to synchronize computer clocks, Network Time Protocol (NTP) is highly favored by [company name] as it requires a reference clock for defining true and accurate time, is fault-tolerant, highly-scalable, and uses trusted external sources (such as UTC). Moreover, NTP's hierarchical structure of clocks, where each level is termed a "stratum", has proven to be a trusted and reliable source for time synchronization. And because the Windows Time Service is not considered to be an accurate measurement of time, other time synchronization technologies are to be implemented. The "Time Synchronization" policy and procedures document, **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package)** which discusses time synchronization policies and procedures for all [company name] system resources, must also include provisions for Citrix XenServer systems.

Access Rights

Access rights to Citrix XenServer systems are limited to authorized personnel only, with all end-users being properly provisioned in accordance with [company name]'s documented access rights policies and procedures. **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package).** This includes using all applicable provisioning and de-provisioning forms as necessary along with ensuring users' access rights incorporate Role Based Access Control (RBAC) protocols or similar access control initiatives.

Additionally, users with elevated and/or super user privileges, such as system administrators, I.T. engineers and other applicable personnel, are responsible for ensuring access rights for all users (both end users and users with elevated and/or super user privileges) are commensurate with one's roles and responsibilities within [company name].

Thus, the concepts of "separation of rights" and "least privileges" are to be adhered to at all times by [company name] regarding access rights to Citrix XenServer systems. Specifically, "separation of rights" implies that both the "functions" within a specified system resource, for which there are many, should be separated along with the roles granted to end-users and administrators of these very system resources. "Functions" pertains to the actions a system resource and its supporting components (i.e., the OS and applications residing on the server) can perform and the associated personnel who have authority over

these functions. Thus, when permissible, functions (such as read, write, edit, etc.) should never be grouped together and end-users and administrators should not be granted access to multiple functions.

By effectively separating access rights to Citrix XenServer systems whereby only authorized individuals have access to the minimum rights needed to perform their respective duties, [company name] is adhering to the concept of "least privileges", a well-known and best practices rule within information technology.

Furthermore, passwords used by all users must meet or exceed all stated [company name] policies for password complexity requirements. Along with ensuring strong passwords, additional password parameters regarding account lockout policies and password resets are also to be enforced with appropriate system settings. Furthermore, only authorized personnel are allowed to make any changes to the password complexity rules and lockout policies to Citrix XenServer systems.

Remote Access

All access to Citrix XenServer systems initiated outside the organization's trusted network infrastructure is to be considered "remote access", and as such, only approved protocols are to be used for ensuring that a trusted connection is initiated, established and maintained. Specifically, all users are to utilize approved technologies, such as IPSec and/or SSL Virtual Private Networks (VPN) for remote access, along with additional supporting measures, such as Secure Shell (SSH), while also employing two-factor authentication. The concept of two-factor authentication (i.e., something you know, something you have, something you are) along with strong password policies creates yet another layer of security relating to access rights for all authorized users granted remote access into [company name's] network.

Additionally, all workstations (both company and employee-owned) are to have current, up-to-date anti-virus software installed, while also utilizing any other malware utilities as needed for protecting the workstations and the information traversing to and from the remote access connection. This may also include the use of personal firewall software, along with enhanced operating system settings on the applicable workstations. The "Remote Access" policy and procedures document, **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package)** which discusses remote access rights policies and procedures for all [company name] system resources, must also include provisions for Citrix XenServer systems.

Malware

Malicious software (malware) poses a critical security threat to Citrix XenServer systems, thus effective measures are to be in place for ensuring protection against viruses, worms, spyware, adware, rootkits, trojan horses, and many other forms of harmful code and scripts. As such, [company name] is to have anti-virus (AV) solutions deployed on all Citrix XenServer systems, with the applicable AV being the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans as necessary. Because strong and comprehensive malware measures are not just limited to the use of AV, additional tools are to be employed as necessary for eliminating all other associated threats, such as those discussed above. The seriousness of malware and its growing frequency of attacks within organizations requires that all I.T. personnel within [company name] stay abreast of useful tools and programs that are beneficial in combating harmful code and scripts. The "Malware" policy and procedures document, **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package)** which discusses anti-malware provisions and related

policies and procedures for all [company name] system resources, must also include provisions for Citrix XenServer systems.

Change Control | Change Management
Changes made to configuration settings (i.e., operating system and application(s) changes) within Citrix XenServer systems require authorized users to initiate an incident and/or change request, which includes completing all applicable forms as necessary. Furthermore, the request must be thoroughly documented, which includes providing the following essential information: (1). An assigned I.D. or change tracking number. (2). Representation of all critical dates relating to the requested change itself, such as when the change was originally submitted and approved, as well as when it was migrated to various stages for testing and final deployment to production, if applicable. (3). Default fields for categorizing (i.e., normal change or emergency change, etc.) and prioritizing (i.e., critical to routine maintenance) the requested change itself. (4). Documented notation, communication and correspondence throughout the life of the requested change itself is to include, but is not limited to, the following: (a). Documentation of impact. (b). Management signoff. (c). Operational functionality. (d). Back-out procedures.

Additionally, change control measures include changes undertaken for any of the following four (4) environments for which Citrix XenServer systems reside in:

- Change Control | Internally Developed Systems and Applications: These include changes made to internally developed platforms for which Citrix XenServer systems are utilized, such as specialized software applications.
- Changes Control | Enterprise Wide: These include changes made to corporate system resources for which Citrix XenServer systems are utilized. This may include file servers or many other types of platforms that are relied upon for the corporate network to function.
- Change Control | Customer Facing Environments: If applicable, these include changes made to customer environments for which Citrix XenServer systems are utilized. This may include specific platforms and portals that are managed by [company name] specifically for customers.
- Emergency Change Management | All Environments: These include emergency changes undertaken for any specific environment (i.e., both client and customer related) for which Citrix XenServer systems are utilized.

The "Change Management" policy and procedures document, **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package)** which discusses change controls policies and procedures for all [company name] system resources, must also include provisions for Citrix XenServer systems.

Patch Management
All necessary system patches and system updates for Citrix XenServer systems (those defined as critical from a security perspective) are to be obtained and deployed in a timely manner as designated by the following software vendor and/or other trusted third-parties: (1). Vendor websites and email alerts. (2). Vendor mailing lists, newsletters and additional support channels for patches and security. (3). Third-party websites and email alerts. (4). Third-party mailing lists. (5). Approved online forums and discussion panels. Effective patch management and system updates help ensure the confidentiality, integrity, and availability (CIA) of systems from new exploits, vulnerabilities and other security threats.

Additionally, all patch management initiatives are to be documented accordingly, which shall include information relating to the personnel responsible for conducting patching, list of sources used for obtaining patches and related security information, the procedures for establishing a risk ranking for patches, and the overall procedures for obtaining, deploying, distributing, and implementing patches specifically related to Citrix XenServer systems. The "Security Patch Management" policy and procedures document, **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package)** which discusses security and patch management policies and procedures for all [company name] system resources, must also include provisions for Citrix XenServer systems.

Backup and Storage

Data backup and storage procedures for Citrix XenServer systems are to be initiated by authorized I.T. personnel consisting of documented processes and procedures that include the following initiatives: (1). The type of backup performed (i.e., full, incremental, and differential backups). (2). The date(s) and time(s) for the designated backup processes to commence. (3). The appropriate reporting procedures and related output for confirmation of backups (i.e., log reports, email notification, etc.). (4). Incident response measures in place for backup failures and/or exceptions. (5). Retention periods for all data backups as required by management, customers, and all necessary regulatory compliance mandates. Additionally, when data has been compromised due to any number of reasons, appropriate restore procedures are to be enacted that allow for complete, accurate, and timely restoration of the data itself.

The "Backup and Storage" policy and procedures document, **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package)** which discusses backup, storage, and archival policies and procedures for all [company name] system resources, must also include provisions for Citrix XenServer systems.

Encryption

When necessary and applicable, appropriate encryption measures are to be invoked for ensuring the confidentiality, integrity, and availability (CIA) of Citrix XenServer systems and any sensitive data associated with them. Additionally, any passwords used for accessing and/or authentication to the specified system resource are to be encrypted at all times, as passwords transmitting via clear text are vulnerable to external threats. As such, approved encryption technologies, such as Secure Sockets Layer (SSL) | Transport Layer Security (TLS), Secure Shell (SSH), and many other secure data encryption protocols are to be utilized when accessing the specified system resource.

Event Monitoring

Comprehensive auditing & monitoring initiatives for Citrix XenServer systems are to be implemented that effectively identify and capture the following events: (1). All authentication and authorization activities by all users and their associated accounts, such as log on attempts (both successful and unsuccessful). (2). Any creation, modification or deletion of various types of events and objects (i.e., operating system files, data files opened and closed and specific actions, such as reading, editing, deleting, printing). (3). All actions undertaken by system administrators who have elevated privileges and access rights.

Additionally, for each event described above, the following attributes are to be captured: (1). The type of event that occurred and on what system level and/or application level did it occur on. (2). The date and

time of the event. (3). The identity of the user, such as the log-on ID. (4). The origination of the event. (5). The outcome of the event, such as the success or failure of the event. (6). The name of the affected system.

Configuration and Change Monitoring

Furthermore, the use of specialized software, such as File Integrity Monitoring (FIM), Host based Intrusion Detection Systems (HIDS), and/or change detection software programs are to be implemented for monitoring Citrix XenServer systems as they provide the necessary capabilities for assisting in the capture of all the above-stated, required events. Additionally, configuration change monitoring tools are to be used to detect any file changes made within a specified system resource, ranging from changes to commonly accessed files and folders, to more granular based data, such as configuration files, executables, rules, and permissions. Changes made are to result in immediate alerts being generated with appropriate personnel being notified. Moreover, these tools effectively aid in capturing and forwarding all events in real-time, thus mitigating issues relating to native logging protocols, which can be accessed by users with elevated privileges on the Citrix XenServer systems themselves, resulting in the disabling and modification of its services and the resulted output.

Performance and Utilization Monitoring

Additional measures are to be employed for ensuring that Citrix XenServer systems are actively being monitored for all necessary performance and utilization measures, such as the following:

- CPU Utilization-Identifies current, real-time capacity of the CPU, and provides alerting and notification measures regarding capacity limits along with underutilization metrics.
- Memory Utilization-Identifies current, real-time memory usage and provides alerting and notification measures if memory usage is high and/or if memory availability is low.
- Disk Utilization-Identifies current, real-time disk space and provides alerting and notification measures if disk space is low.
- Process Monitoring-Monitors all critical processes and provides alerting and notification measures when processes fail.
- Network Interface Monitoring-Monitors the overall health and status of the network interface.

Authorized personnel are to appropriately configure all Citrix XenServer systems for ensuring the aforementioned measures are in place via tools that provide agent based monitoring, the use of native agents on the specified system resource itself, along with agentless monitoring, if applicable.

Logging and Reporting

Along with capturing all necessary events as described in "Event Monitoring", effective protocols and supporting measures are to be implemented for ensuring all required events and their associated attributes are logged, recorded, and reviewed as necessary. Additionally, all applicable elevated permissions (those for administrators) along with general access rights permissions (those for end-users) to Citrix XenServer systems are to be reviewed on a [monthly/quarterly/bi-annual/annual] basis by an authority that is independent from all known users (i.e., end-users, administrator, etc.) and who also has the ability to understand, interpret, and ultimately identify any issues or concerns from the related output (i.e., log reports, and other supporting data). The specified authority reviewing the logs is to determine what constitutes any "issues or concerns", and to report them immediately to appropriate personnel.

Moreover, protocols such as syslog and other capturing and forwarding protocols and, or technology, such as specialized software applications, are to be used as necessary, along with employing security measures that protect the confidentiality, integrity, and availability (CIA) of the audit trails and their respective log reports (i.e., audit records) that are produced. Additionally, all audit records are to be stored on an external log server (i.e., centralized syslog server or similar platform) that is physically separated from the original data source, along with employing effective backup and archival procedures for the log server itself. These measures allow [company name] to secure the audit records as required for various legal and regulatory compliance mandates, along with conducting forensic investigative procedures if necessary.

Incident Response

[Company name] has in place documented incident response initiatives, which includes provisions for effectively preparing, detecting, responding, and recovering from an incident, along with initiating post-incident activities and awareness. Thus, these five (5) provisions, which are discussed in detail within the "Incident Response Plan" documentation, **(Note: The referenced document can be purchased separately, or if you've purchased the entire collection of templates, it's included as part of the package)** are to also consist of the following measures for incidents relating to Citrix XenServer systems:

1. "Preparing" in that employees and all other applicable parties should be aware of security threats and computer incidents and undertake all necessary and required training.
2. "Detecting" in that procedures are in place that allow for timely detection of all threats, such as the use of specific software tools and other monitoring and detection elements.
3. "Responding" in that procedures are in place that allow for rapid and swift response measures, which is highly necessary for containing and quarantining any given incident.
4. "Recovering" in that procedures are in place that allow for full recovery of the affected systems, such as the use of backup media and the ability to rebuild, reconfigure and redeploy as necessary.
5. "Post Incident Activities and Awareness" in that a formal and documented Incident Response Report (IRR) is to be developed, reviewed by appropriate parties, resulting in "Lessons Learned" from the incident and what initiatives can be implemented for hopefully eliminating the likelihood of future incidents.

These measures form a critical component of ensuring the protection of the organization's network infrastructure, and as such, are to be immediately implemented when an incident arises that may affect the security of Citrix XenServer systems

Performance and Security Testing

Citrix XenServer systems are to undergo annual vulnerability assessments along with penetration testing for ensuring their safety and security from the large and ever-growing external and internal security threats facing [company name] today. Vulnerability assessments, which entails scanning a specified set of network devices, hosts, and their corresponding Internet Protocol (IP) addresses, helps identify security weaknesses within [company name's] network architecture, along with those specifically related to Citrix XenServer systems. Additionally, penetration testing services, which are designed to actually compromise the organization's network and application layers, also assists in finding security flaws that require immediate remediation. Moreover, contractual requirements along with regulatory compliance laws and legislation often mandate organizations perform such services, at a minimum, annually (for penetration tests), and often on a periodic and/or quarterly basis (for vulnerability assessments). As such, [company

name] will adhere to these stated requirements and will perform the necessary services on Citrix XenServer systems.

Careful planning and consideration of what systems are to be included when performing vulnerability assessments and, particularly penetration testing, is a critical factor, as all environments (i.e., development, production, etc.) must be safeguarded from any accidental or unintended exploits caused by the tester.

Additionally, if [company name] has internally developed, proprietary applications (i.e., software) residing on Citrix XenServer systems, appropriate code reviews are to be conducted for ensuring the software itself has been coded and developed with the appropriate security measures. Poorly coded software, specifically software used for web facing platforms, can be compromised through numerous harmful tactics, such as Cross-site scripting (XSS), injection flaws (SQL, etc.) and other damaging methods.

Disaster Recovery

Documented Business Continuity and Disaster Recovery Planning (BCDRP) is vital to protecting all [company name] assets along with ensuring rapid resumption of critical services in a timely manner. Because disasters and business interruptions are extremely difficult to predict, it is the responsibility of authorized [company name] personnel to have in place a fully functioning BCDRP process, and one that also includes specific policies, procedures, and supporting initiatives relating to all system resources, including Citrix XenServer systems.

1.0 Procedures

[Company name] has developed and implemented a comprehensive Citrix XenServer systems security and hardening process, which encompasses the following categories and supporting activities listed below. These policy directives will be fully enforced by [company name] for ensuring the Citrix XenServer systems security initiatives are executed in a formal manner and on a consistent basis for all specified systems.

Note: The "Policy" sections contained within this specific policy and procedure document simply state general best-of-breed practices that should be in place. However, the "Procedures" sections list and describes the actual steps to undertake for ensuring compliance with the aforementioned policies. As such, look upon the policies as statements, formal guidelines, and the general framework for a particular subject matter. As for the procedures, these are the actual processes, steps, workflow activities and supporting initiatives that illustrate how the actual policies are implemented. In summary, policies state what are to be done, while procedures show you how they are done.

Additionally, if you want to provide any more information that's relevant to each section listed below, please use the “Additional Information” box [shown under each section], as this allows you to document any additional evidence of the procedures undertaken for meeting adherence with the stated policies. All information in light blue text should be deleted as this information is merely stated for reference purposes.

Data and Information Classification Procedures

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding data information and classification for the specific system resource. Thus, please use the "Procedures" section to actually describe various specifics pertaining to data and information classification. For example, you should discuss what data and information classification initiatives you have in place, etc. Lastly, please discuss what other supporting policies, procedures, or processes are in place regarding data and information classification procedures for this specific system resource].

Additional Information
General Notes | Comments:

Security Categorization Procedures

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding security categorization for the specific system resource. Thus, please use the "Procedures" section to actually describe various specifics pertaining to security categorization. For

example, you should discuss what security categorization initiatives you have in place, etc. Lastly, please discuss what other supporting policies, procedures, or processes are in place regarding security categorization procedures for this specific system resource].

Additional Information
General Notes | Comments:

Physical Security Procedures

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding physical security for the specific system resource. Thus, please use the "Procedures" section to actually describe various specifics pertaining to physical security. For example, you should discuss the location of the specific system resource, physical security controls in place, etc. Lastly, please discuss what other supporting policies, procedures, or processes are in place regarding physical security procedures for this specific system resource].

Additional Information
General Notes | Comments:

Personnel Procedures

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding the personnel responsible for provisioning and maintaining the specific system resource. Thus, please use the "Procedures" section to actually describe various specifics pertaining to personnel for ensuring they are competent and qualified employees. For example, you should discuss the various titles, roles and responsibilities of personnel assigned to provisioning and maintaining the specific system resource and their applicable skill sets, etc. Lastly, please discuss what other supporting policies, procedures, or processes are in place regarding personnel procedures for this specific system resource].

Additional Information
General Notes | Comments:

Security Awareness Training Procedures

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding security awareness and training for the specific system resource. Thus, please use the "Procedures" section to actually describe what "procedures" are undertaken. For example, you should discuss security awareness training that is specific to this system resource, such as training measures

undertaken, etc. Lastly, please discuss what other supporting policies, procedures, or processes are in place regarding security awareness training for this specific system resource].

Additional Information
General Notes | Comments:

Provisioning and Hardening Procedures

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding provisioning and hardening for the specific system resource. Thus, please use the "Procedures" section to actually describe what "procedures" are undertaken. For example, you should discuss the use of hardening documents that are vendor specific, websites that are visited for additional hardening information, etc. Lastly, please discuss what other supporting policies, procedures, or processes are in place regarding provisioning and hardening for this specific system resource].

Additional Information
General Notes | Comments:

Time Synchronization Procedures

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding time synchronization for the specific system resource. Thus, please use the "Procedures" section to actually describe what "procedures" are undertaken. For example, you should discuss how the specific system resource obtains the overall time synchronization readiness. Lastly, please discuss what other supporting policies, procedures, or processes are in place regarding time