*Cloud Information Security*

General System Secure Configuration Baseline Standards

**Supplemental to Information Technology Corporate Standard (ITCS) 104**

© 2017 IBM. All Rights Reserved.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| version | Date | APPROVED BY | Description of the Change |
| 0.1 | 19-Oct-2016 |  | Initial draft |
| 0.2 | 19-Oct-2016 |  | Document registered, headers updated |
| 0.3 | 27-Oct-2016 | Penny Leigh Poe | Policy Management Review, Edit and Comment  SME Accepted changes – Requesting SOP Notification for Publishing |
| 1.0 | 02-Nov-2016 | Tim Brophy | Approved for publishing |
| 1.1 | 16-Nov-2016 |  | Change from FEDR to CONF document – applies to both federal and commercial environments |
| 1.2 | 08-Dec-2016 |  | Submit for approval |
| 2.0 | 03-Jan-2017 | Tim Brophy | Approved for publishing |
| 2.1 | 23-Oct-2017 |  | Project Bluenote Update (template, verbiage to IBM) |
| 2.2` | 1-Nov-2017 |  | Policy Management Update |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 1](#_Toc495476017)

[1.1 Purpose 1](#_Toc495476018)

[1.2 Scope 1](#_Toc495476019)

[1.3 Triggers and Outputs 2](#_Toc495476020)

[2 Procedures 3](#_Toc495476021)

[2.1 (Example)Firewall ACL Procedures 3](#_Toc495476022)

[2.1.1 Add Firewall ACL 3](#_Toc495476023)

[2.1.2 Delete Firewall ACL 4](#_Toc495476024)

[3 Tables and Figures Style Guide 5](#_Toc495476025)

[3.1 Tables 5](#_Toc495476026)

[3.2 Figures 5](#_Toc495476027)

[3.2.1 Full-width Figure 5](#_Toc495476028)

[4 Responsibility 6](#_Toc495476029)

[5 Exceptions 6](#_Toc495476030)

[6 Expiration 6](#_Toc495476031)

[7 Enforcement 6](#_Toc495476032)

[8 Appendices 7](#_Toc495476033)

[Appendix A - Terms and Definitions 8](#_Toc495476034)

[Appendix B - References 9](#_Toc495476035)

[Appendix C - Distribution 10](#_Toc495476036)

List of TABLES

[Table 3‑1: TableTitleLine Style 5](#_Toc495476037)

[Table 3‑2: TableTitleLine Style 5](#_Toc495476038)

[Table A‑1: Terms and Definitions 8](#_Toc495476039)

[Table B‑1: References 9](#_Toc495476040)

[Table C‑1: Distribution Contacts 10](#_Toc495476041)

List of Figures

[Figure 2‑1: Figure Title 3](#_Toc495476042)

[Figure 2‑2: Figure Title 3](#_Toc495476043)

[Figure 2‑3: Figure Title 4](#_Toc495476044)

[Figure 2‑4: Figure Title 4](#_Toc495476045)

[Figure 3‑1: Figure Title 5](#_Toc495476046)

1. **Overview**

## Purpose

This Standard documents the addendum Standards and Requirements supplemental to IBM Global Technology Services (GTS) Cloud Transformation Services (formerly Verizon), hereinafter referred to as “GCTS.”

This document details the minimum set of security requirements for all servers or devices within the GCTS environment. Applying the security controls included in this document helps minimize the likelihood of a successful compromise of these IT assets by an attacker. GCTS increases its assurance that these systems and the data they contain will be appropriately secured from the loss of confidentiality, integrity and availability.

## Scope

The security controls described in this document apply to any device connected to the GCTS network. The operating system or device specific secure configuration baseline standard document should be referenced instead of this document. This document applies in cases when an operating system or device specific secure configuration baseline standards document is not available.

The procedures detailed in this document apply to all GCTS full and part-time employees, temporary workers, volunteers, contractors, or any other agents employed to perform work and who have been granted access to GCTS information systems and information assets.

The term ”IBM” referenced in this document is representative of any brand or location where IBM operates, to include, but not limited to:

* IBM Managed Hosting (MH)
* IBM Enterprise Cloud Managed Edition (ECME)
* IBM Remote Applications Management (RAM)
* IBM GCTS
* IBM IP Applications Hosting (IPAH)
* IBM infrastructure

All requests for exclusions to controls identified within this document must be must be approved by the GCTS Business Owner (BO) or Information Resource Custodian (IRC) of record as defined by the governing/serving Lightweight Enterprise Governance Organization (LEGO) as defined by LEGO Program Charter and the LEGO Knowledge Management Charter.

Requirements:

Check the GCTS Document Management System (DMS) for a secure configuration baseline standard document (SCB) which matches the operating system or device. This document should only be used if an operating system or device specific SCB does not exist in DMS.

## General System Security

### General Configuration Requirements

1. Deploy system with current software version. Promptly apply patches when notifications of software bugs and/or security vulnerabilities are announced by the vendor.
2. User or administrative access to a system must be authenticated against an external user database using LDAP, Kerberos, RADIUS or TACACS+.
3. Local user accounts are only to be used in a case when there is a network connectivity failure between the server/device and external authentication server.
4. Unused ports, services and daemons must be disabled or removed to prevent unauthorized execution.
5. Obfuscate the default Simple Network Management Protocol (SNMP) community string. Must not be based on dictionary words; must be minimum of fourteen (14) characters and contain at least three (3) of the following four (4) classes:
6. Upper case letters (e.g., A, B, C, …Z)
7. Lower case letters (e.g., a, b, c, …z)
8. Westernized Arabic numerals (e.g., 1, 2,3, …9)
9. Non-alphanumeric (special characters) (e.g., ?, ! %, $, #, etc.)
10. Restrict SNMP access to authorized internal monitoring servers and/or subnets.
11. SNMP must be disabled if it is not required.
12. Logging must be configured. Refer to System Logging and Access List Logging Best Practices (SECM-00446).
13. The configuration of any production system must be limited to the minimum authorized network services, protocols, and bindings necessary for operation.
14. All systems and other network elements capable of Network Time Protocol (NTP) synchronization must be synchronized to an NTP time server derived from a Global Positioning System (GPS) receiver or equivalent time source.
15. Disable wireless (wifi) when not in use.
16. When wireless (wifi) is enabled on a system all other network connectivity must be disabled or disconnected.
17. Wireless (wifi) Ad hoc mode is not permitted and must be disabled.
18. Any system configured with wireless capabilities must have host-based firewall turned on whenever wireless is enabled.
19. Any system directly interacting with a human user must allow user-initiated screen saver and keyboard locking.
20. The screen saver or keyboard unlock procedure must require user re-authentication after 10 minutes of inactivity.
21. Each device must display an IBM approved banner at the time of user authentication. Please refer to section 2.2 of [SECM-00286 Login Warning Message Policy.docx](https://urldefense.proofpoint.com/v2/url?u=http-3A__blueoperationsportal.apps.tmrk.corp_Quality-2520Management_Drafted-2520Documents_TCC-2520Drafts_SECM-2D00286-2520Login-2520Warning-2520Message-2520Policy.docx&d=DwMFAg&c=jf_iaSHvJObTbx-siA1ZOg&r=Ww47Y4ZM0xX9g9xxPZcjxsQ2aXW1eqgHbeBTIe_k-ko&m=7tWsvYv_hq9yFlAALcu-FAGqWzzpRZocf5qdL4kJvdI&s=g8B-EgX5Z8IYCYRhUFRUmFLjUXUzmLPaq3wQgQnI2fI&e=).
22. Disable DHCP server.
23. Disable IPv6 when not in required or in use.
24. Outbound Internet access must be restricted to a web proxy.

#### System Logging

Refer to [SECM-00446 System Logging and Access List Logging Best Practices](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00446%20System%20Logging%20and%20Access%20List%20Logging%20Best%20Practices.pdf).

#### System Access

Refer to [SECM-00153 Access Control Policy](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00153%20Access%20Control%20Policy.pdf).

#### User Accounts and Passwords

Refer to [SECM-00153 Access Control Policy](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00153%20Access%20Control%20Policy.pdf).

#### Secure Transport Protocols

All new builds must use only TLSv1.2 or higher. SSLv3, TLSv1, TLSv1.1 should be disabled. Only high level perfect forward secrecy ciphers should be utilized; or just list the ciphers as high level encryption ciphers with perfect forward secrecy ciphers preferred.

Refer to [SECM-00369 Secure Transport Protocols-TLS Hardening](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00369%20Secure%20Transport%20Protocols-TLS%20Hardening.pdf).

#### Login Warning Message/Banner

Refer to [SECM-00286 Login Warning Message Policy](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00286%20Login%20Banner%20Policy.pdf).

## Servers

In addition to the general controls identified in *Section 1.3*, devices functioning as a server will be held to controls identified within this section. This section includes general controls which apply to all servers. Additionally, this section includes controls based on the server’s role. Both the general server controls and the appropriate specific controls are required.

1. Test/development servers must be maintained on physically separate host platforms from production servers.
2. Servers intended for internal use only must not be located in a DMZ network and may not be accessed from the Internet.
3. Database servers may not be located within DMZ networks.
4. Direct interactive (human) login to a service account is prohibited and must be disabled using whatever technical measures, if any, are provided by the underlying system.
5. System configuration information must never be accessible via remote file sharing.
6. Host firewalls must be enabled, and all blocked packets must be logged.

An Operational Global Exception exists for this control if traffic is filtered by a stateful inspection based network firewall. For questions please contact [GCTS\_Cloud\_SecurityOps@wwpdl.vnet.ibm.com](mailto:GCTS_Cloud_SecurityOps@wwpdl.vnet.ibm.com)

1. Host firewalls must restrict externally initiated connections except for those required for the application(s) running on the host and serve a specific business need.

An Operational Global Exception exists for this control if traffic is filtered by a stateful inspection based network firewall. For questions please contact [GCTS\_Cloud\_SecurityOps@wwpdl.vnet.ibm.com](mailto:GCTS_Cloud_SecurityOps@wwpdl.vnet.ibm.com)

1. Host firewalls must be configured so that administrative access is restricted to approved internal networks.

An Operational Global Exception exists for this control if traffic is filtered by a stateful inspection based network firewall. For questions please contact [GCTS\_Cloud\_SecurityOps@wwpdl.vnet.ibm.com](mailto:GCTS_Cloud_SecurityOps@wwpdl.vnet.ibm.com)

1. Anti-virus software must be installed and enabled. Virus definition updates should be regularly.
2. File integrity monitoring software must be installed and enabled.
3. Disable IP forwarding.
4. Disable ICMP redirects.
5. Configure server to ignore ICMP broadcasts.

### Server Specific Controls

#### Linux Servers

1. Disable unused filesystems
   * cramfs
   * freevxfs
   * jffs2
   * hfs
   * hfsplus
   * squashfs
   * udf
   * FAT
2. Create separate partition for /tmp.
3. Set nodev, nosuid, and noexec options on /tmp partition.
4. Create separate partition for /var.
5. Create separate partition for /var/tmp or bind-mount /tmp as /var/tmp
6. Set nodev, nosuid, and noexec options on /var/tmp partition.
7. Create separate partition for /var/log.
8. Create separate partition for /var/log/audit.
9. Create separate partition for /home.
10. Set nodev, nosuid, and noexec options on /dev/shm partition.
11. Set nodev, nosuid,and noexec options on removable media partitions.
12. Disable automounting (autofs).
13. Configure package manager GPG keys.
14. Restrict access to core dumps.
15. Enable address space layout randomization (ASLR).
16. Disable unnecessary services:
    * Chargen
    * Daytime
    * Discard
    * Echo
    * Time
    * Rsh-server (rsh, rlogin, rexec)
    * Talk
    * Telnet server
    * TFTP server
    * Xinetd
    * FTP server
17. Ensure X Window System is not installed.
18. Ensure Avahi Server is not enabled.
19. Ensure CUPS is not enabled.
20. Ensure file deletion events by users are collected.
21. The syslog daemon must be configured to start automatically at boot time.
22. Log changes to sudoers file.
23. Log system administrator’s actions.
24. Any world-writable directory must have the sticky bit set.
25. Ensure cron daemon is enabled.
26. The permissions on crontab entries must be read/write for owner and no access for group or others.
27. Crontab entries must not be invoked or referenced from world readable/writable files.
28. Accounts with elevated privileges that run scripts and programs must not be owned by or reside in a user level home directory.
29. Shadow password file access must be restricted to the local administrator account or to processes running as root.
30. Server must be configured with SSH protocol version 2 only.
31. Disable uncommon network protocols.

For example:

* + Datagram Congestion Control Protocol (DCCP)
  + Stream Control Transmission Protocol (SCTP)
  + Reliable Datagram Sockets (RDS)
  + Transparent Inter-Process Communication (TPIC)

#### Windows Servers

1. Remove or rename default administrator account.
2. Remove or disable the default guest account.
3. “Access this computer from the network” user right must be assigned to a more restrictive group compared to older operating system defaults, which uses groups such as Everyone, Authenticated Users or Domain Users.
4. Configure ‘Act as a part of the operating system’ to ‘No one’.
5. On domain controllers, ensure ‘add workstations to domain’ setting is set to ‘administrators’.
6. Ensure ‘adjust memory quotas for a process’ is set to ‘administrators, local service, network service’.
7. Configure ‘allow log on locally’ as follows:
8. Domain controller: Administrators, Enterprise Domain Controllers
9. Member server: Administrators
10. Configure ‘allow log on through Remote Desktop Services’
11. Domain controller: Administrators
12. Member server: Administrators, Remote Desktop Users
13. Ensure ‘back up files and directories’ is set to ‘administrators’
14. Ensure ‘change the system time’ is set to ‘administrators, local service’.
15. Ensure ‘change the time zone’ is set to ‘administrators, local service’.
16. Ensure ‘create a pagefile’ is set to ‘administrators’.
17. Ensure ‘create a token object’ is set to ‘no one’.
18. Ensure ‘create global objects’ is set to ‘administrators, local service, network service, service’.
19. Ensure ‘create permanent shared objects’ is set to ‘no one’.
20. Set ‘create symbolic links’ to ‘administrators’.
21. Ensure ‘debug programs’ is set to ‘administrators’.
22. Ensure ‘deny log on as a batch job’ to include ‘guests’.
23. Ensure ‘deny log on as a service’ to include ‘guests’.
24. Ensure ‘log on locally’ to include ‘guests’.
25. Configure ‘enable computer and user accounts to be trusted for delegation’
26. Domain controller: Administrators
27. Member server: No one
28. Ensure ‘force shutdown from a remote system’ is set to ‘administrators’.
29. Enable setting ‘Network access: Do not allow storage of passwords and credentials for network authentication’.
30. Ensure ‘allow LocalSystem NULL sessions fallback’ is set to disabled.
31. Configure server to prevent the ability of anonymous users to enumerate SAM accounts and shares.
32. Configure the “LAN Manager Authentication Level” security option to “Send NTLMv2 response only. Refuse LM & NTLM”.
33. Disable the ability to store LAN Manager password hashes within the local user account database.
34. Restrict the ability to shut down the server to appropriate administrators only.
35. Require users to log on to the server in order to shut down the server. (Disable ‘do not require CTRL+ALT+DEL and disable “allow system to be shut down without having to log on’).
36. Do not display username of last user account that logged in.
37. Require ‘minimum session security for NTLM SSP (including secure RPC) clients’ to ‘Require NTLMv2 session security, Require 128bit encryption’.
38. Require ‘minimum session security for NTLM SSP (including secure RPC) servers’ to ‘Require NTLMv2 session security, Require 128bit encryption’.
39. Service accounts must be audited in the same manner as user accounts.
40. Enforce security settings on Windows servers using Group Policy.
41. Turn off Windows Error Reporting.
42. Disable Remote Assistance.
43. Prevent collection of anonymous information by Microsoft by disabling customer feedback or customer experience improvement program, and other similar programs.

#### Web Servers

1. The web server process must not run as the system administrator account.
2. Create a dedicated physical disk or logical partition for web content. The physical disk or logical partition must be separate from the Operating System (OS) and the web server application.
3. Remove or disable services installed by the web server that is but not required (e.g. FTP, SMTP, and Internet Printing).
4. Configure the web server process to run as a user with a limited set of privileges.
5. Server hardware running multiple web server instances (virtual web servers) must be configured so that each web server instance supports its own logging.
6. Remove or disable unnecessary services, applications, and sample content, including scripts and executable code.
7. Access to web-based administrative tools such as webadminpwd, webadminconf, IIS Remote Administration (HTML) Tool, must be either removed or restricted to authorized systems administrators and TLS protected.
8. Script interpreters, (e.g. Perl), must not reside in a directory that is published by the web server (e.g. cgi-bin).
9. Web servers must not display the source code of any server-side executable content, including, but not limited to Active Server Pages (ASP), Common Gateway Interface (CGI), Professional Home Pages (PHP), Perl, and Java.
10. Web server must be configured to only execute CGI scripts that reside in authorized CGI binary directories.
11. Ownership and permissions on the CGI common directory must be set such that only the web server administrator account can create CGI script programs.
12. Servers must be configured to disallow the “~” (home directory) option.
13. Automatic generation of directory listings (Apache option “Indexes”; IIS setting “Directory Browsing”) must not be enabled on a global basis. Automatic directory listing may optionally be enabled in specific directories, at the discretion of the web server administrator, provided that all of the following criteria are met:
14. The directories contain no server –side executable content.
15. The directories contain no source code to any server-side executable content.
16. The directories contain no server configuration data or server log files.
17. The directories prohibit write access by all user or process, to include the web server process UserID, except the web server administrator.
18. Server-side includes are permitted only for web pages which have been reviewed and determined safe.
19. Symbolic links within the web server directory structure must be disabled.
20. Explicit path names must be used when invoking external programs from within CGI scripts server-side executable content (CGI, ASP).
21. When use of the PATH environment variable is required in a script, it must be set at the beginning of the script to prevent damage from subverted scripts.

#### Virtual Servers

1. Virtualization must not introduce new communication paths between security zones or trust boundaries that would not otherwise exist in a non-virtualized architecture.
2. User-facing applications must not reside on the host system (e.g. hypervisor).
3. Shared files and file systems between guest operating systems must be minimized and must never cross network segments of differing security zones.
4. Promptly install software updates to guest operating system, as well as, applications running on the guest operating system.
5. In each guest OS, disconnect unused virtual hardware (e.g. network adapters, serial and parallel ports, CD and floppy drives).

#### Hypervisors

1. Secure access to the hypervisor by restricting access to the management interfaces (e.g. SSH, HTTPS) to authorized internal IP address or networks.
2. The management interface (e.g. SSH or HTTPS) of the host operating system (hypervisor) must not be accessible to the virtual machines.
3. The management interface (e.g. SSH or HTTPS) of the host operating system (hypervisor) must not be accessible to the virtual machines.
4. Routinely install software updates on the hypervisor.
5. Disable hypervisor file sharing services or file sharing services between the hypervisor and VMs (guest OS).

## Network Device Controls

### General Network Device Specific Controls

1. A dedicated management interface (if available) must be used for administrative access.
2. Administrative (e.g. console port, management port, SSH) access to the device must be restricted to authorized internal networks.
3. All administrative access must require a password.
4. The device must have an inactivity timeout configured for all administrative access (e.g. console and SSH). Refer to section 2.1.1.2 System Access.
5. Change the vendor default password(s).
6. All unused or unnecessary services must be disabled. (e.g. Dynamic Host Configuration Protocol (DHCP), source routing, small services, finger, X.25 PAD).
7. Disable insecure or unnecessary protocols (e.g. identd)
8. The device must not be configured to reply to ICMP broadcasts.
9. All administrative commands must be logged and stored on a separate system if the network device has the ability to support remote logging. Refer to section 2.1.1.1 System Logging.
10. The network device configuration must be backed up to an external system.
11. Network device configuration files must be stored on a system with a hardened operating system.
12. Access to the backup repository should be restricted to only those who require access to perform their job responsibilities.
13. Trivial File Transfer Protocol (TFTP) may not be used to automatically load configuration file and IOS at reboot unless needed to temporarily fix a network problem. A TFTP server must reside on a protected internal network.
14. Logging must be enabled on each interface access list entry.
15. The last entry in any interface access list must include an explicit deny rule. Additionally, this rule must have logging enabled.
16. Access lists applied to a network device interface must not include an entry which has an undefined source and destination (e.g. permit ip any any).
17. Configure reverse path filtering.

# Responsibility

The GTCS BO or IRC of record is responsible and held accountable for enforcement of published policy, process, and procedure documentation.

It is the responsibility of all personnel to know, understand, and conform to the policies set in the ITSC 104, Business Conduct Guidelines, World-Wide Records Management, and others as they apply to all GCTS employees

# Exceptions

must be approved by the GCTS BO or IRC of record as defined by the governing/serving Lightweight Enterprise Governance Organization (LEGO) as defined by LEGO Program Charter and the LEGO Knowledge Management Charter.

# Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Appendices

Appendix A - Terms and Definitions 8

Appendix B - References 9

Appendix C - Distribution 10

Appendix - Terms and Definitions

Table A‑1: Terms and Definitions

| Term | Definition |
| --- | --- |
| ASP | Active Server Pages |
| BO | Business Owner |
| CGI | Common Gateway Interface |
| DHCP | Dynamic Host Configuration Protocol |
| DMS | Document Management System |
| DMZ | Demilitarized Zone |
| ECME | Enterprise Cloud Managed Edition |
| FTP | File Transfer Protocol |
| GCTS | Global Technology Services (GTS) Cloud Transformation Services (formerly Verizon) |
| GPS | Global Positioning System |
| GRCQ | Governance of Risk, Compliance, and Quality |
| GTS | Global Technology Services |
| HTMP | Hyper Text Markup Language |
| HTTPS | Hyper Text Transfer Protocol Secure |
| ICMP | Internet Control Messaging Protocol |
| IP | Internet Protocol |
| IPAH | IP Applications Hosting |
| IRC | Information Resource Custodian |
| ITCS | Information Technology Corporate Standards |
| LDAP | Lightweight Directory Access Protocol |
| LEGO | Lightweight Enterprise Governance Organization |
| MH | Managed Hosting |
| NSB | Network Security Baseline |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Professional Home Pages |
| RADIUS | Remote Authentication Dial-in User Service |
| RAM | Remote Applications Management |
| SCB | Secure Configuration Baseline |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| TACACS+ | Terminal Access Controller Access-Control System Plus |
| TFTP | Trivial File Transfer Protocol |

Appendix - References

Table B‑1: References

| Document Number | Document Title |
| --- | --- |
| CIO 122 | IBM Worldwide Records Management |
| CIS Linux Benchmark | [CIS Distribution Independent Linux Benchmark v1.0.0](https://benchmarks.cisecurity.org/tools2/linux/CIS_Distribution_Independent_Linux_Benchmark_v1.0.0-CC.pdf) |
| CIS Windows Server 2012 R2 Benchmark | [CIS Microsoft Windows Server 2012 R2 Benchmark](https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf) |
| IBM BCG | IBM Business Conduct Guidelines |
| ITCS 104 | IBM Information Technology Corporate Standard 104 |
| NIST 800-125 | [NIST 800-125 Guide to Security for Full Virtualization Technologies](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf) |
| NIST 800-41 rev1 | [NIST 800-41 Guidelines on Firewalls and Firewall Policy](http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf) |
| NIST 800-44 version 2 | [NIST 800-44 version 2 - Guidelines on Securing Public Web Servers](http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf) |
| SECM-00153 | [Verizon Cloud Services Access Control Policy](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00153%20Access%20Control%20Policy.pdf) |
| SECM-00286 | [Login Warning Message Policy](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00286%20Login%20Banner%20Policy.pdf) |
| SECM-00369 | [Secure Transport Protocols-TLS Hardening](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00369%20Secure%20Transport%20Protocols-TLS%20Hardening.pdf) |
| SECM-00446 | [System Logging and Access List Logging Best Practices](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00446%20System%20Logging%20and%20Access%20List%20Logging%20Best%20Practices.pdf) |

Appendix - Distribution

Table C‑1: Distribution Contacts

| Name/Role | Contact Information |
| --- | --- |
| Document Management | [Document.Management@verizon.com](mailto:Document.Management@verizon.com); Document\_Management@wwpdl.vnet.ibm.com |
| Fed Compliance | [GCTS-FedCompliance@wwpdl.vnet.ibm.com](mailto:GCTS-FedCompliance@wwpdl.vnet.ibm.com) |
| Roger Gaffey | [gafferog@us.ibm.com](mailto:gafferog@us.ibm.com) |
| Shannon Soland | [solansha@us.ibm.com](mailto:solansha@us.ibm.com) |
| Scott Owenby | [owenbsco@us.ibm.com](mailto:owenbsco@us.ibm.com) |
| GCTS Security Operations Team | [GCTS\_Cloud\_SecurityOps@wwpdl.vnet.ibm.com](mailto:GCTS_Cloud_SecurityOps@wwpdl.vnet.ibm.com) |