Network Security Standard

In accordance with Information Security Policy

Published: 3/11/2019

Document Owner: Chris Nims - Paranoids

TABLE OF CONTENTS

©2019,Verizon Media Inc. A Verizon company

OBJECTIVE

To establish a standard related to network security for Verizon Media and its affiliates as to day to day operations and support of Verizon Media Information Security policies and controls. This document addresses security protections related to network security by identifying specific requirements that network devices, administration and procedures must meet.

This standard provides security requirements for network security, which promotes the overall security of Verizon Media and its affiliates.

SCOPE

This document is intended for use by all Verizon Media employees, contractors, vendors, and partners handling Verizon Media data.

This standard applies to all IT systems and applications connected to Verizon Media Information Infrastructure, or otherwise utilized by Verizon Media, including, but not limited to, physical and virtual servers, cloud-based hosts (such as AWS), databases, desktops, laptops, mobile phones, tablets, network devices, wireless access points, audio-visual, telephony, operating system software, supporting software, application code and supporting infrastructure services.

SUMMARY

This standard addresses the security of Verizon Media networks. This encompasses generalized requirements, minimum security configuration development, firewall, segmented networks, VPN, remote access, wireless networks, monitoring, review, implementation, and documentation of those requirements.

This security standard expands upon, and is in accordance with, the Verizon Media Information Security Policy.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

CONTROLS

GUID	Control Name	Control Description	Requirement Details
General Network Protections			
AC.H.16	Network Switches - Trust Zone Access	All requests for access to Verizon Media Information Resources must be reviewed and approved by the Paranoids, Paranoids approved automated processes, or managed using group membership in cloud infrastructure. All transitions between network boundaries or zones occur through securely managed network paths or via Paranoids approved mechanisms.	Network zones of greater trust requires additional security controls including access reviews
AC.H.103	Network Availability and Integrity	Network availability must be protected. This includes available bandwidth as well as services necessary to facilitate network operation.	Secure fundamental network availability and the services that allow network communication (i.e. NTP, DNS, routing protocols, routers, etc.). As well as monitoring the Internet for the misuse of our public address space.
AC.H.11	Dual Homing and NAT Restrictions	Systems and Information Assets must reside inside single network zones unless an authorized exception for bridging between zones is acquired.	Bridging two networks incurs significant risk, due to the additional attack surface and potential for user behaviour to affect systems deemed critical to business operations.
AC.H.18	Administrative Access	Jumphosts or bastion hosts must be used for all system administration in the Verizon Media environment.	“Bastion hosts” may also refer to ssh proxy/gateways that have been reviewed and approved by Paranoids.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

AC.H.19	Other Forms of Internet Access	Alternate forms of Internet access, such as dial-out modems, DSL, and ISDN lines must not be used inside Verizon Media networks unless approved by the Paranoids prior to implementation and use.	Networks that have not been approved by The Paranoids will most likely be configured with poor security, and potentially allow unauthorized parties access to the Verizon Media environment.
Network Device Configuration - Minimum Security Baseline			
IP.A.06	Document and Create Network Security Architecture	A secure network security architecture for the enterprise/BU/specific environment must be developed and documented following the requirements defined in the Requirement Details.	This network security architecture must: 1. Describe the overall requirements and approach to be taken with regard to protecting the confidentiality, integrity, and availability of information; 2. Describe how the network security architecture is integrated into and supports the enterprise architecture; and 3. Describe any information security assumptions about, and dependencies on, external services.
IP.W.01	Service Protocols	Prior to implementation with the Verizon Media network, the network configuration requirements defined in the Requirement Details must be deployed for device management.	No unauthorized connections from public infrastructure can be used for device management: 1. Cleartext protocols, Telnet, HTTP, and any unused services must be disabled for device management on all network equipment. 2. TFTP must be restricted to device configuration automation servers only for backup and maintenance purposes. 3. Where required, encrypted protocols such as HTTPS

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

			and SSH must be enabled based on business need. 4. Unused services must be disabled on Network Devices. 5. Unused interfaces must be disabled following the completion of the deployment of Network Devices.
AC.H.101	Network Device Administration - SNMP Community Strings	If SNMP is in use then all network device administration must be performed using only corporate standardized SNMP community strings. SNMPv3 must be enabled for device monitoring on all network equipment.	Secure SNMP usage requires enabling and configuring SNMPv3. It should also be used in combination with management information base (MIB) whitelisting using SNMP views. In addition, using different and complex SNMP strings to devices of different security levels is good practice.
AC.H.102	Network Device Administration - Logging	All activity performed on network devices must be logged and audited.	None
Network Device Configuration - Device Access			
IP.Y.02	Admin Hosts - Management Access	Management access to network devices must be restricted to authorized administrative hosts and networks through the use of access controls.	Only administrative hosts and networks, specifically authorized by Paranoids are granted management privileges.
IP.Y.05	Inactivity Timeout	Logon sessions for network devices must be set to automatically disconnect after 1 hour of inactivity.	All logon functions should be set for a default inactivity timer of 1 hour, after which idle connections must be automatically terminated.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

AC.H.21	Network Time Protocol	Network devices must be synchronized with Paranoids approved Network Time Protocol (NTP) servers.	Time synchronization is critical for accurately capturing when events occur. Root cause analysis depends on accurate timestamping.
Network Device Configuration - Access Filtering			
IP.V.02	Routing Updates	Updates to network device routing tables, must be pushed or distributed from approved, authenticated devices only.	None
Change Management			
AC.H.30	Firewall Changes and Exceptions	Changes and proposed exceptions to network device firewalls, including AWS Security Groups and host-based firewalls, must be approved and follow a documented change management procedure per Verizon Media's Change Management Policy.	Change management process requires at a minimum a review of the changes and how it impacts the organization. The impact should take into consideration whether those changes violates Verizon Media policies or standards. A common example of this are firewall changes which allow for opening up firewall ports from the Internet.
Firewalls			
AC.H.25	Firewall Placement	Firewalls must be in place and operational between the networks and devices outlined in the Requirement Details section of this control	The network locations where Firewalls are required are: 1. Between the Verizon Media network and the public network; 2. Between any Demilitarized Zone (DMZ) and any internal network; 3. Between any sensitive network zone and wireless access points.
AC.H.27	Management Access	Firewalls must drop or reject any management traffic	None

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

		directed at the firewall other than from approved firewall management stations.	
AC.H.28	Firewall Configuration Backup	All firewall configurations and rule sets must be backed up as per local disaster recovery plans.	Having a recent backup of the firewall configuration can save time not only during a crash but also during problems with new policy configuration changes when you need to revert the firewall to all the settings of an earlier configuration. With a backup you can perform the restoration as a single operation instead of manually re-configuring each setting in the current configuration.
AC.H.29	Allowed Traffic Justification	All traffic allowed through the firewalls must have a business purpose that is justified and documented.	This documentation must contain the following: ● Service/Protocol Allowed (including TCP and UDP port number) ● Description of the Service ● Business Rationale for the Service
AC.H.35	Firewall Network Address Translation	Inbound Network Address Translation must not be used without approval from Paranoids. Source routing must be disabled for all firewalls and external routers.	Network Address Translation (NAT) is designed for IP conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. As part of this capability, NAT can be configured to advertise only one address for the entire network to the Internet, effectively hiding the entire internal network behind that address.
AC.H.38	Administrator Periodic Training	Firewall administrators must receive periodic training on the firewalls in use and in network security principles and	Periodic training helps ensure that personnel also gets the most up to date information to effectively manage these

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

		practices at least once every two years, so that firewalls are configured correctly and administered properly.	evolving devices.
AC.H.04	Deny by Default	Access to Information Resources must fail securely in the event of an operational failure of a network zone protection device. Verizon Media network communications traffic must be denied by default and allowed only by a formal approval process from the Paranoids. All firewall rules and access policies must operate under the principle of least privilege.	Failures of boundary protection devices must not lead to or cause external information to enter the devices, and must also prevent the release of internal information.
AC.H.07	Firewalls - Rule Base	The rule base for any firewall must follow the minimum requirements outlined in the Requirement Details section of this control.	The minimum requirements for a firewall rule base are as follows: 1. The rule base must be configured according to the principle of least privilege and deny all traffic by default; 2. The rule base must be documented and associated with an authorized change control, and must be validated at least annually.
AC.H.08	Firewalls - Rule Base Review	The functionality of protocols and services defined in the rule base for a firewall must be reviewed and approved annually by the Paranoids during the firewall rule review. Justification and documentation for all requested protocols must be recorded, including reason for use and mitigating controls.	None

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Segmented Networks			
AC.H.02	Network Segmentation - Internal/External	Verizon Media servers accessible from the Internet must be logically isolated from internal use networks by being placed in a demilitarized zone (DMZ) that utilizes publically routable Internet Protocol (IP) space when making or receiving connections to the public Internet. Network zones must have defined boundaries and be clearly documented.	A Demilitarized Zone holds external Internet-facing servers and resources that are accessible from the Internet while the entirety of the internal network remains unreachable from the Internet. Segregation and systems placement must be based on the data classification, risk compromise, and sensitivity.
Protected Networks			
AC.H.44	Network Segmentation - Confidential Data	Protected networks must be established to limit access to Verizon Media Confidential data.	Protected networks are often needed to create a logical network separation from the general use network through some type of boundary protection such as firewall, router ACL, or host ACL. By doing so, the organization can define various levels of access to the protected systems based on business need. Access is generally not allowed by default unless specifically requested.
AC.H.50	Direct Internet Connection	Protected networks and assets hosted in protected networks must not connect to the Internet directly, unless using Paranoids approved mechanisms.	Various factors must be assessed before considering connecting protected networks directly to Internet. This include applicable laws, regulations and contractual obligations.
Office Networks			
AC.H.53	Network Segmentation - Office Networks	Office networks are logically separated from other network zones, including Demilitarized Zones (DMZs) and protected	End-user computing devices generally are more susceptible to compromise due to the various ways these devices are used.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

		networks.	These include Internet browsing and connecting to untrusted networks such as hotels, home networks, and wifi hotspots. Exposure to various threats may subject the rest of the organizational assets to additional risk unless they are mitigated.
Transit Networks			
AC.H.57	Routing Peer Authentication	All authentication methods used by routing peers must be approved by the Paranoids before routing peers accept routes. This authentication method must be annually reviewed and approved by the Paranoids.	Router authentication enables routers to share information only if they can verify that they are talking to a trusted source. This can be done through various ways including the use of hashed key, or a keychain.
AC.H.58	Third Party Transit Network Connections	All requests for third party connections to transit networks, as well as requests for extranet access, are approved by the business owner of the third party relationship, Paranoids, and the network organization.	Transit networks allow traffic from one network to cross or “transit” to another network.
Development and Test Networks			
AC.H.59	Production Access Requests	All requests for access from a development or test network to production must be reviewed and approved before being granted.	Access review and approval is more than just trust or potential for unauthorized developer access to critical production information. It also allows for the reviewer to ensure there is separation of data, code and activities between these separate environments.
Routing			

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

AC.H.09	Routing Information Propagation	Routing information must not be propagated to an untrusted network unless deemed necessary for a business function.	Alternatives to sharing network routing information should be evaluated to determine the minimal set of information that needs to be shared for the business function.
AC.H.62	Anti-IP Spoofing	Filtering must be implemented on all border routers to protect against IP address spoofing.	IP spoofing is the creation of IP packets which have a modified source address in order to hide the identity of the sender, to impersonate another computer system or both. It is commonly used for two reasons in DDoS attacks: to mask botnet device locations and to stage a reflected assault. It is also used to bypass security measures that rely on IP blacklisting.
IP.V.01	Anti-Spoofing	Controls must be implemented to prevent spoofing of Verizon Media IP space, or unintentional leaking of private or internal IP addresses.	Inbound traffic must not have a source IP address of an internal network, or a reserved private IP address. This is enforced through access control list configurations on network perimeter routers.
Virtual Private Network (VPN)			
AC.H.66	VPN Implementations	All VPN solutions and architectural designs are reviewed and approved by the Paranoids before implementation. Once implemented, Virtual Private Network connections must be reviewed at least annually by the Paranoids.	A VPN is an extension of a private network so that remote users or a physically separated network can communicate to the internal network over the Internet. It is imperative to define who can use the VPN, what it can be used for, and the security policies that prevent improper or malicious use. Considerations must be given to the potential vulnerabilities of VPN. This include Man in the middle (MITM), DDOS, and SSL trusted

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

			certificate authority hack.
Domain Name Services			
AC.H.79	Approved Name Resolution	Name resolution must be performed using only approved authoritative and recursive DNS servers.	There are various types of attacks that can compromise DNS servers. This includes DNS cache poisoning. This can happen after an attacker is successful in injecting malicious DNS data into the recursive DNS servers that are operated by many ISPs. Another is when attackers take over one or more authoritative DNS servers for a domain. Lastly, an attacker can compromise the registration of the domain itself, and then use that access to alter the DNS servers assigned to it.
Wireless Networks			
AC.H.82	Approved Wireless Connectivity	Wireless connectivity to Verizon Media networks must be through Paranoids approved solutions. All wireless access points and base stations connected to the corporate network are registered and approved by Paranoids. Mechanisms must be in place to prevent the implementation of individual wireless access points for the purpose of connecting to an Verizon Media internal or corporate network.	Implementation of wireless access points by individuals jeopardizes the established network segmentation.
AC.H.85	Wireless Access Requirements	Processes and procedures must be developed and documented to include the wireless access requirements defined in the Requirement	Usage restrictions and implementation requirements must be established and documented prior to the implementation of new wireless

©2019 Verizon Media, Inc. A Verizon company

		Details. The requirements must be implemented to prevent misuse of wireless access, whether accidentally or intentionally.	networks, including the following considerations: 1. Wireless networks that do not require user authentication (ie. Guest Networks or Extended-Stay) must not allow access to corporate information resources and should be restricted to internet access only. 2. Wireless networks that provide access to corporate information systems must protect access to those systems using authentication of users and devices, and encryption.
AC.H.86	SSID Information Disclosure	Wireless SSIDs must be configured such that it does not disclose any identifying information about the organization, such as the company name, division title, employee name, or product identifier.	Making sure corporate wireless networks are configured in endpoint devices alleviates the need to use descriptive SSID.
Malicious Code and Spam Protection			
AC.H.89	Malicious Code Protection	Malicious code protection mechanisms (including signature definitions) must be implemented and update-to-date at the Office Network entry and exit points to detect and eradicate malicious code.	One of the most effective ways to stop harmful content getting into the corporate network via the Internet is to stop it at the gateway level of the network. With the proper network architecture, gateway protections can help ensure malware cannot enter or leave the corporate network, and real-time protection against malware on email, on websites and during file transfers.
AC.H.91	Spam	Spam protection mechanisms	Simply put, spam is unsolicited

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

	Protection	must be employed for email.	e-mail. They are usually advertisements, but sometimes they are scams, attempting to entice a person to divulge account information (such as username and passwords). To help prevent spam from reaching and leaving corporate mailboxes, email security gateways manages and filters all inbound and outbound email traffic. Spam filtering methods can include using list-based (blacklist, whitelist, greylist), content-based, word-based, heuristic and bayesian filters.
Monitoring and Troubleshooting			
AC.H.93	Central Network Monitoring System	A network monitoring system must be used to monitor the integrity and availability of the network.	None
Documentation			
AC.H.96	Network Environment Documentation	Network environment documentation must be centrally stored and made available to supporting personnel.	None

ROLES AND RESPONSIBILITIES

General Network Protections

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that all transitions between network boundaries or zones occur through securely managed network paths such as Security Groups with NACLs or via Paranoids/Network Security approved mechanisms (AC.H.16)

Production Support Shall:

a. Ensure that information assets are only connected between network boundaries or zones according to business requirements and risk (AC.H.11)

Net Protect Shall:

a. Implement and monitor Network availability and Integrity methods such as DDOS detection, alerts etc.(AC.H.103)

Paranoids shall:

a. Ensure that systems are not bridged between network zones unless there is an authorized exception (AC.H.11)
b. Ensure that all requests for access within the Verizon Media network are reviewed and approved by Paranoids or managed using group membership in cloud infrastructure (AC.H.16)
c. Provide requirements for Network availability and Integrity such as DDOS detection, alerts etc. (AC.H.103)

All Users shall:

a. Ensure that no other form of internet access such as dial-out modems, DSL, analog and ISDN lines, are used inside Verizon Media network unless approved by Paranoids (AC.H.19)

Data Custodians/DBA/SA shall:

a. Ensure that system administration are not performed on hosts in production environments directly from the Verizon Media office network, corporate VPN or any other connectivity. System administration of Verizon Media production environment use jumphosts or 'bastion' hosts (AC.H.18)
b. Ensure that all data entering protected networks are reviewed and approved by Paranoids before being passed from a lower security network zone to a higher security network zone (AC.H.16)

Network Operations and Lead Architects shall:

a. Ensure that all data entering protected networks are reviewed and approved by Paranoids before being passed from a lower security network zone to a higher security network zone (AC.H.16)

Network Device Configuration - Minimum Security Baseline

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Custodians/DBA/SA shall:

a. Ensure that network device ports and interfaces are disabled when not in use, unless approved by Paranoids (IP.W.01)

Paranoids shall:

a. (For custodians of information security controls) Develop an information security architecture for their specific environment (IP.A.06)

Network Teams and Lead Architects shall:

a. Ensure that the Secure Shell protocol or an out-of-band management system is required to access network devices (IP.W.01)
b. Ensure that Telnet, HTTP, HTTPS and any unused services are disabled for device management on all network equipment, and that TFTP is to be restricted only to device configuration automation servers for backup and maintenance purposes (IP.W.01)
c. (For custodians of security controls) Develop an information security architecture for their specific environment (IP.A.06)
d. Ensure that network device ports and interfaces are disabled when not in use, unless approved by Paranoids (IP.W.01)
e. Ensure that no local user accounts are configured on routers. Only corporate standardized SNMP community strings, that follow Access Control Standard, are used. Authentication, authorization and accounting (AAA) is used. All activities performed on the routers are logged and audited (AC.H.102)
f. Ensure that, prior to implementation onto the Verizon Media network, SSH is enabled for device management and SNMPV3 is enabled for device monitoring on all network equipment (AC.H.101)

Network Device Configuration - Device Access

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Custodians/DBA/SA shall:

a. Ensure that logon sessions are set to disconnect after 15 minutes of inactivity by default (IP.Y.05)

©2019 Verizon Media, Inc. A Verizon company CONFIDENTIAL

Network Teams and Lead Architects shall:

a. Ensure that management access to network devices are restricted to authorized administrative hosts and networks (IP.Y.02)
b. Ensure that access lists are enabled to restrict SSH access (IP.Y.02)
c. Ensure that console logon sessions are set to disconnect after 15 minutes of inactivity by default (IP.Y.05)
g. Ensure that network devices are synchronized with approved Network Time Protocol (NTP) servers (AC.H.21)

Network Device Configuration - Access Filtering

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Network Operations and Lead Architects shall:

a. Restrict connections such that only limited authenticated devices have the ability to push updates to network devices (IP.V.02)

Change Management

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that changes or proposed exceptions to network devices, including AWS Security Groups or host-based firewalls, are approved and follow a documented change management procedure per the Change Management Request process (AC.H.30)

Firewalls

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media. and any applicable subsidiaries

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that all firewall configurations and rule sets are backed up as per local disaster recovery plans (AC.H.28)
b. Ensure that firewall administrators receive periodic training on the firewalls in use and in network security principles and practices, so that firewalls are configured correctly and administered properly (AC.H.38)

Net Protect Shall:

a. Ensure that firewalls are installed and operating between the public network and Verizon Media network, between any DMZ and internal network, and between any sensitive network zone and wireless access points (AC.H.25)
b. Ensure that boundary protection deny network traffic by default and allow network traffic based on business need (AC.H.04).
c. Ensure that firewall rule, access policies, and security protections for each network boundary/zone are defined based on the principles of least privilege and deny all by default and access to Information Resources fails securely in the event of an operational failure of a network zone protection device (AC.H.04)
d. Ensure that Verizon Media network communications traffic is denied by default and allowed by a formal approval process from governing information security organization (i.e., deny all, permit by exception) (AC.H.04)
e. Ensure that for a filtering device (e.g. firewalls), all rules within its rule base are restricted to only allow the appropriate traffic, documented and associated with an authorized change control and reviewed and validated annually (AC.H.07)
f. Ensure that defined protocols and services are analyzed as part of a risk assessment effort during firewall rule review and that the justification and documentation for all requested protocols are recorded including reason for use and mitigating controls (AC.H.08)
g. Record the justification and documentation for all requested protocols including reason for use and mitigating controls (AC.H.08)

Network Operations Team shall:

a. Ensure that firewall drops or rejects any management traffic directed at the firewall other than from approved firewall management stations (AC.H.27)
b. Ensure that all allowed traffic through a firewall has a justified business purpose and are documented (AC.H.29)
c. Ensure that firewalls are configured such that all Information Resource User Internet network traffic appears as if the traffic had originated from the firewall (i.e. only the firewall address is visible to outside networks, NAT) (AC.H.35)

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

d. Ensure that outbound Network Address Translation (NAT) and proxy are only permitted via the Paranoids approved means (AC.H.35)

Custodian/DBA/SA shall:

a. Ensure that firewall drops or rejects any management traffic directed at the firewall other than from approved firewall management stations (AC.H.27)
b. Ensure that all allowed traffic through a firewall has a justified business purpose and are documented (AC.H.29)

Segmented Networks

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Network Operations and Lead Architects shall:

a. Ensure that Information Resources which are accessed from external networks are logically isolated from networks intended only for internal use (AC.H.02)

Global Network Infrastructure Services shall:

b. Ensure network zones or boundaries, including cloud infrastructure, are defined. Systems are defined and maintained within specific network boundaries or zones (AC.H.02)

Custodian/DBA/SA shall:

a. Ensure that Information Resources which are accessed from external networks are logically isolated from networks intended only for internal use (AC.H.02)
b. Ensure that Verizon Media network communications traffic is denied by default and allowed by a formal approval process from governing information security organization (i.e., deny all, permit by exception) (AC.H.04)

Network Operations Team shall:

a. Ensure that Verizon Media network communications traffic is denied by default and allowed by a formal approval process from governing information security organization (i.e., deny all, permit by exception) (AC.H.04)

Protected Networks

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

©2019 Verizon Media, Inc. A Verizon company

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Network Operations and Lead Architects shall:

b. Ensure that protected networks are established to limit access to Verizon Media Confidential data and applications (AC.H.44)
c. Ensure that protected networks must not connect directly to the Internet unless via Paranoids approved mechanisms (AC.H.50)
d. Ensure that direct connections from the Internet to assets hosted in protected networks are prohibited unless via Paranoids approved mechanisms (AC.H.50)

Custodian/DBA/SA shall:

a. Ensure that protected networks must not connect directly to the Internet unless via Paranoids approved mechanisms (AC.H.50)
b. Ensure that direct connections from the Internet to assets hosted in protected networks are prohibited unless via Paranoids approved mechanisms (AC.H.50)

Office Networks

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Network Operations and Lead Architects shall:

a. Ensure that office networks logically separated from other network zones, including Demilitarized Zones (DMZs) and protected networks. (AC.H.53)

Transit Networks

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that all routing peers use an approved method of authentication before accepting routes and are periodically reviewed (AC.H.57)
b. Ensure that third party connections to transit networks are approved by the business

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

owner of the third party relationship, Paranoids and Global Network Infrastructure Services (GNIS) (AC.H.58)

Custodian/DBA/SA shall:

a. Ensure that third party connections to transit networks are approved by the business owner of the third party relationship, Paranoids and Global Network Infrastructure Services (GNIS) (AC.H.58)

Development and Test Networks

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Net Protect Shall:

a. Ensure that all requests for access from a development and test network to production are reviewed and require approval (AC.H.59)

Custodian/DBA/SA shall:

a. Ensure that all requests for access from a development and test network to production are reviewed and require approval (AC.H.59)

Routing

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that private routing information will only be disclosed to third party for necessary business functions (AC.H.09)

Network Operations and Lead Architects shall:

a. Ensure that filtering is implemented to protect against IP address spoofing (AC.H.62)
b. Ensure that filtering is implemented to protect against Verizon Media IP space (IP.V.01)
c. Ensure that, prior to implementation onto the Verizon Media network, SSH is enabled for device management and SNMPV3 is enabled for device monitoring on all network equipment (AC.H.101)

Net Protect Shall:

©2019 Verizon Media, Inc. A Verizon company

a. Ensure that filtering is implemented to protect against IP address spoofing (AC.H.62)
b. Ensure that filtering is implemented to protect against Verizon Media IP space (IP.V.01)

Custodian/DBA/SA shall:

a. Ensure that private routing information will only be disclosed to third party for necessary business functions (AC.H.09)

Virtual Private Network (VPN)

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that all requests for VPN connections are reviewed and approved by Paranoids. (AC.H.66)
b. Ensure that VPN connections are periodically reviewed by Network Security (AC.H.66)

Custodian/DBA/SA shall:

a. Ensure that all requests for VPN connections are reviewed and approved by Paranoids. (AC.H.66)
b. Ensure that VPN connections are periodically reviewed by Paranoids. (AC.H.66)

Domain Name Services (DNS)

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Network Operations and Lead Architects shall:

a. Ensure that only approved authoritative and recursive DNS servers are used for name resolution (AC.H.79)

Wireless Networks

Chief Technology Officer (CTO) shall:

©2019 Verizon Media, Inc. A Verizon company

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that all wireless Access Points / Base Stations connected to the corporate network are registered and approved by Global Network Infrastructure Services (GNIS) (AC.H.82)
b. Ensure that enterprise networks establish usage restrictions and implementation guidance for wireless access, authorize wireless access to corporate information resources prior to connection and protect wireless access to the system using authentication of users and devices, and encryption (AC.H.85)

Network Operations and Lead Architects shall:

a. Ensure that wireless connectivity to Verizon Media are through a Paranoids approved solution (AC.H.82)

Network Operations shall:

a. Ensure that the non-Guest wireless SSID are configured following the Passwords section of the Access Control Standard, so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier (AC.H.86)

Custodian/DBA/SA shall:

a. Ensure that all wireless Access Points / Base Stations connected to the corporate network are registered and approved by Global Network Infrastructure Services (GNIS) (AC.H.82)

All Information Resource Users shall:

a. Ensure that all wireless Access Points / Base Stations connected to the corporate network are registered and approved by Global Network Infrastructure Services (GNIS) (AC.H.82)

Malicious Code and Spam Protection

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

©2019 Verizon Media, Inc. A Verizon company

Global Network Infrastructure Services shall:

a. Ensure that malicious code protection mechanisms at the Office Network entry and exit points to detect and eradicate malicious code are employed (AC.H.89)
b. Ensure that spam protection mechanisms are employed (AC.H.91)

Network Operations shall:

a. Ensure that gateway malicious code protection mechanisms (including signature definitions) are updated whenever new releases are available (AC.H.89)

Monitoring and Troubleshooting

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Network Automation shall:

a. Ensure that a central network monitoring system are used to monitor the integrity and availability of the network (AC.H.93)

Documentation

Chief Technology Officer (CTO) shall:

a. Be ultimately responsible for the correct and thorough management of network security throughout Verizon Media and any applicable subsidiaries

Chief Information Security Officer (CISO) shall:

a. Advise the CTO on the completeness and adequacy of network security efforts and documentation to ensure compliance to this Standard
b. Review and approve or disapprove all new Standard and Control changes

Global Network Infrastructure Services shall:

a. Ensure that documentation of the network environment are available to the Paranoids, all network teams, or other analysis related teams (AC.H.96)

DEFINITIONS

Access	Action performed by any user or process to enter, utilize, or manipulate a system, network, dataset, right or privilege with respect to an Information Resource.

©2019 Verizon Media, Inc. A Verizon company

Access Device	A device (e.g., access card, key, key fob, ID card, hardware token) that grants the possessor the ability to gain access to Verizon Media's facilities or information resources.
Asset Custodian	Verizon Media employee designated as the principal point of contact for an information resource other than an application. The individual is accountable for maintaining the asset record and for the management and implementation of the Information Resource's security requirements.
Authentication	The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: ● Something the user knows, such as a password or PIN ● Something the user has, such as a smartcard or ATM card ● Something that is part of the user, such as a fingerprint or iris
Business Owner	A Business Owner (BO) is responsible for the function or purpose served by an Information Resource and is responsible for understanding business functions and business requirements (Some Information Resources may serve an IT purpose only). A BO is a VP level, or equivalent responsibility employee (or higher) within the organization responsible for the Information Resource. The BO is also responsible for awareness of any special conditions, requirements or restrictions applicable to the data and for communicating information as appropriate. A BO may delegate its responsibility to an individual employee within its management chain, Director level, or equivalent responsibility, however the BO remains fully accountable.
BU / Corp Function	Refers to any managed function (at the corporate or BU-level) including but not limited to IT, HR, Legal, as opposed to an individual responsibility.
CISO	Chief Information Security Officer is responsible information security strategy, policies, standards, architecture and processes.
CTO	Chief Technology Officer is responsible for overseeing and developing the company's strategy for using technological resources.
Change vs Maintenance	Any planned deviation from the previously agreed upon configuration, which typically requires a formal approval (e.g. through change management process). A maintenance activity is not necessarily a change.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Commercial off the Shelf (COTS) Software	Software which is available in the commercial marketplace and can be purchased and used in accordance with licensing terms and conditions.
Configuration Baseline	Agreed upon configuration requirements/settings designed to balance security and operational needs.
Cryptographic Erase	A method of sanitization in which the Media Encryption Key (MEK) for the encrypted target data (or the Key Encryption Key – KEK) is sanitized, making recovery of the decrypted target data Infeasible.
Data Loss Prevention (DLP)	A strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe security solutions that help a network administrator control what data end users can transfer.
Data masking	Data masking (also known as data obfuscation, data scrubbing, and data scrambling) involves concealing parts of information (e.g., names, addresses, social security numbers and credit card numbers).
Data Overwrite	Writing data on top of the physical location of data stored on the media. This method can be used as a means of "data destruction", when the original data needs to be destroyed. Data overwriting will replace the original data with gibberish, making the original data unreadable.
Data truncation	Data truncation refers to restricting the number of characters that is displayed or printed from the original stream of sensitive data.
Dedicated Paranoids	Security champions for their designated teams. They can serve in several capacities such as: help to make decisions about when to engage the Paranoids, act as the "voice" of security for the given product or team, assist in the triage of security bugs for their team or area.
Database Admin (DBA)	Provides technical support for the development, maintenance, security and troubleshooting of database configurations and functionality.
Denial of Service	An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.
DSL	Digital Subscriber Line is a technology for providing network access at high speeds to homes and businesses over ordinary public

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

	switched telephone network.
DMZ	A part of the network that is neither part of the internal network nor directly part of the Internet. A firewall or a router usually protects this zone with network traffic filtering capabilities and isolates from internal networks.
Encryption	The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.
Extranet	A private network that uses the Internet protocols and the public telecommunication system to securely share part of a business' information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.
Firewall	A hardware or software solution that limits access between networks in accordance with local security policy.
Full Disk Encryption	When every data block on the storage medium (except for bootstrap areas) is encrypted with a Verizon Media-approved encryption method.
Information Custodians / Technology Owners	Individuals (e.g., IT staff) who maintain or administer Information Resources on behalf of Information Owners.
Information Owners / Data Owners	The individuals ultimately responsible for Information Resources, and are generally Departmental Vice Presidents or designated senior managers.
Information Resource	Any Verizon Media owned or contracted data, communication, computing device or technology which may include, but is not limited to: applications, application infrastructure elements, application programming interfaces (APIs), bots, databases, file systems, operating systems, networks, network infrastructure elements, printouts, data, graphics, access cards, keys, key fobs, workstations, mobile devices, servers, IoT devices, control systems, drones, virtual machines, middleware, code libraries, and other similar or related elements that store, process, transmit and/or display Verizon Media data.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Information Resource User	An individual that can access, utilize, modify, or otherwise manipulate Verizon Media Information Resources.
Information Infrastructure	The collection of systems and networks relative to Information Resources where Verizon Media information/data is stored or processed.
ISDN	Integrated Services Digital Network is an international standard for end-to-end digital transmission of voice, data, and signaling over ordinary telephone copper wire.
Least Privilege	The access control principle that requires Verizon Media Responsible Parties to maintain end-users access only to those Verizon Media Information Resources and the associated rights and privileges to those resources as is required to perform their duties.
Lead Architects	The group responsible for planning / architecting the technical network solutions and overall structure.
Maintenance	A variety of activities (e.g., diagnostics, physical repair, replacement, physical move) that are required to keep physical assets: servers, industrial or facility controllers (e.g. HVAC), network components etc. running properly. Unlike a formal change, maintenance activity is intended to preserve functional status quo while addressing operational shortcomings.
Minimum Security Baseline	Agreed upon configuration requirements/settings designed to meet a set of minimum security requirements while balancing operational needs.
Media Destruction	A method of media sanitization (e.g. shredding) that renders target data recovery unfeasible using advanced techniques. Following the media destruction process, the media in question is no longer capable of storing data.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Network Operations	The group which performs the daily network support, maintenance and troubleshooting activities.
Network Device	Any physical component which forms part of the underlying connectivity infrastructure for a network
Net Protect	The team that support firewalls and manages firewall ACLs.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Net Planning (Network Planning)	The group responsible for planning / architecting the technical network solutions and overall structure.
NetOps (Network Operations)	The group which performs the daily network support, maintenance and troubleshooting activities.
Verizon Media Information	All information that is rightfully obtained, developed, or produced by or for Verizon Media and/or its employees as part of Verizon Media business activities. Used synonymously with the terms 'information', 'data' and 'Verizon Media Data'.
Verizon Media Information Assets	Data/information owned, used, stored, processed or transmitted by Verizon Media or by its vendors, business partners or other third parties acting on behalf of Verizon Media (collectively “Vendors”), as well as the systems and applications used by Verizon Media to create, process, modify, store, and communicate such information.
[Verizon Media] Confidential	Information that Verizon Media considers sufficiently sensitive to require a minimum set of specific controls in order to reasonably protect the information.
[Verizon Media] Highly Confidential	Special category of “Verizon Media Confidential” information requiring other controls and protections in addition to those needed for “Verizon Media Confidential” information.
[Verizon Media] Private	Information that Verizon Media does not wish to be publicly disclosed, but is protected only through company policies/Code of Conduct, controlled access to Verizon Media facilities and similar common practices.
[Verizon Media] Public	Information that is publicly known or available without restriction.
Non-public data	This refers to data classified as private, confidential or highly confidential.
Paranoids	Group operating under Verizon Media CISO responsible for providing oversight and guidance on the implementation of security risk mitigating controls, tools and procedures, as well as providing security solutions and support..

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Production Support	The collective teams that support Applications, Hardware, System Software, Networks, Security, etc. They may also participate in the Crisis and Availability Management processes by interacting with the Crisis Management Desk (CMD) and Stability & Availability Management (S&AM) teams.
Remote Access	Any access to Verizon Media corporate networks through a network, device, or medium such as the Internet, public phone line, wireless carrier, or other external connectivity that is not controlled by Verizon Media.
Risk	The probability the vulnerability will be exploited multiplied by the impact the exploit will have.
Router	A device or system that finds the best path for data packets between any two networks, even if there are several networks to traverse. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as “routing metrics”. It can be used to filter traffic between two networks.
Security Incident	Any real or suspected activity that violates an explicit or implied security policy.
SSID	Short for service set identifier, a unique identifier that acts as a password on a wireless network.
Switch	A device that connects network segments or computers.
System Administrator	Individual(s) responsible for operational administration of Information Resource(s). Their responsibilities would include upkeep and configuration of information resources to ensure uptime, performance and security of the information resources they manage in line with organizational requirements.
Third Party	A business that is not a formal or subsidiary part of Verizon Media.
Trust Relationship	Trust relationships are an administration and communication link between two domains such as those managed by domain controllers or authentication systems. A trust relationship between two domains enables user accounts and global groups to be used in a domain other than the domain where the accounts are defined.
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

Threat-source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.
Untrusted Network	Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.
VPN	A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.
Vulnerability	Any flaw or weakness in a system or process that may make it susceptible to being used by an unauthorized individual, or group of individuals (accidentally triggered or intentionally exploited), resulting in a violation of an explicit or implied security policy.
WAN	A computer network that spans a relatively large geographical area, consisting of two or more local area networks.
Wireless Access Point	A device that provides radio signal connectivity for wireless LAN clients and a wired-network connection, bridging the wireless and wired networks

NON-COMPLIANCE

Instances of non-compliance with this standard must be documented with justification, using the Executive Risk Evaluation (ERE) process and the associated PSR process, so that the associated risks can be evaluated by the Paranoids, and communicated to business leadership for approval.

RENEWAL

This standard will be reviewed and renewed within one year from the effective date listed in this document.

DOCUMENT ADMINISTRATION

References

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company

- Data Classification Standard
- Secure Logging & Monitoring Standard
- Access Control Standard
- Data Security Standard

Revision Schedule
This standard should be reviewed and updated annually.

Revision History

Version	Revised On	Modified By / Revised By	Description of Change	Approved By	Approved On
1.0	11/28/2018	P&C	First Version	Chris Nims, CISO	3/11/2019

Effective Date: 3/11/2019

Go back to TABLE OF CONTENTS

©2019 Verizon Media, Inc. A Verizon company