VNF Security Requirements (from ONAP)

This page will serve as a placeholder to get the matrix complete and then the Recommended changes will be made to the appropriate documents.

- VNF General Security Requirements
- VNF Identity and Access Management Requirements
- VNF API Security Requirements
- VNF Security Analytics Requirements
- VNF Data Protection Requirements
- VNF Cryptography Requirements

VNF General Security Requirements

	VNF Security Ref	Description	Notes		CNTT Relevant	Exists	CNTT Ref#	Current Description, if exists	Recommended Description (may be a modification of existing)
1	R-118669	Login access (e.g., shell access) to the operating system layer, whether interactive or as part of an automated process, MUST be through an encrypted protocol such as SSH or TLS.			Y	N			All login access (e.g., shell access) to any service, whether interactive or as part of an automated process, **must** be through an encrypted protocol such as SSH or TLS 1.2 or higher.
2	R-19082	The VNF MUST not contain undocumented functionality.							
3	R-19768	The VNF SHOULD support the separation of (1) signaling and payload traffic (i.e., customer facing traffic), (2) operations, administration and management traffic, and (3) internal VNF traffic (i.e., east-west traffic such as storage access) using technologies such as VPN and VLAN.							
4	R-21819	VNFs that are subject to regulatory requirements MUST provide functionality that enables the Operator to comply with ETSI TC LI requirements, and, optionally, other relevant national equivalents.							
5	R-23740	The VNF MUST implement and enforce the principle of least privilege on all protected interfaces.			Y	Y	RA-1 2.3.8.2 Platform and Access sec.sys.007	The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control)	
6	R-240760	The VNF MUST NOT contain any backdoors.							
7	R-256267	If SNMP is utilized, the VNF MUST support at least SNMPv3 with message authentication.							
8	R-258686	The VNF application processes SHOULD NOT run as root. If a VNF application process must run as root, the technical reason must be documented.							
9	R-353637	Containerized components of VNFs SHOULD follow the recommendations for Container Base Images and Build File Configuration in the latest available version of the CIS Docker Community Edition Benchmarks to ensure that containerized VNFs are secure. All non-compliances with the benchmarks MUST be documented.							
10	R-381623	Containerized components of VNFs SHOULD execute in a Docker run-time environment that follows the Container Runtime Configuration in the latest available version of the CIS Docker Community Edition Benchmarks to ensure that containerized VNFs are secure. All non-compliances with the benchmarks MUST be documented.							

11	R-46986	The VNF provider MUST follow GSMA vendor practices and SEI CERT Coding Standards when developing the VNF in order to minimize the risk of vulnerabilities. See GSMA NESAS Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements Version 1.0 (https://www.gsma.com/ security/wp-content/uploads/2019/11/FS.16-NESAS-Development-and-Lifecycle-Security- Requirements-v1.0.pdf) and SEI CERT Coding Standards (https://wiki.sei.cmu.edu/ confluence/display/seccode/SEI+CERT+Coding+Standards).							
12	R-56904	The VNF MUST interoperate with the ONAP (SDN) Controller so that it can dynamically modify the firewall rules, ACL rules, QoS rules, virtual routing and forwarding rules. This does not preclude the VNF providing other interfaces for modifying rules.							
13	R-61354	The VNF MUST provide a mechanism (e.g., access control list) to permit and/or restrict access to services on the VNF by source, destination, protocol, and/or port.							
14	R-62498	The VNF MUST support only encrypted access protocols, e.g., TLS, SSH, SFTP.			Y	Y	RA-1 2.3.8.2 Platform and Access sec.sys.003 (doesn't mention technologies)	The Platform **must** support Secure and encrypted communications, and confidentiality and integrity of network traffic	The Platform **must** support Secure and encrypted communications, and confidentiality and integrity of network traffic, utilising encrypted access protocols such as TLS 1.2 or higher, SSH, SFTP.
15	R-638682	The VNF MUST log any security event required by the VNF Requirements to Syslog using LOG_AUTHPRIV for any event that would contain sensitive information and LOG_AUTH for all other relevant events.							
16	R-69649	The VNF Provider MUST have patches available for vulnerabilities in the VNF as soon as possible. Patching shall be controlled via change control process with vulnerabilities disclosed along with mitigation recommendations.	RA-1 includes requirements for the platform						
17	R-756950	The VNF MUST be operable without the use of Network File System (NFS).							
18	R-80335	For all GUI and command-line interfaces, the VNF MUST provide the ability to present a warning notice that is set by the Operator. A warning notice is a formal statement of resource intent presented to everyone who accesses the system.							
19	R-842258	The VNF MUST include a configuration (e.g. a heat template or CSAR package) that specifies the targeted parameters (e.g. a limited set of ports) over which the VNF will communicate; including internal, external and management communication.							
20	R-86261	The VNF MUST be able to authenticate and authorize all remote access.							
21	R-872986	The VNF MUST store Authentication Credentials used to authenticate to other systems encrypted except where there is a technical need to store the password unencrypted in which case it must be protected using other security techniques that include the use of file and directory permissions. Ideally, credentials SHOULD rely on a HW Root of Trust, such as a TPM or HSM.			Y	Y	RA-1 2.3.8.1 System Hardening sec.gen.003	All servers part of Cloud Infrastructure **must** support a root of trust and secure boot	modify to add, "such as TPM or HSM" as in: All servers part of Cloud Infrastructure **must** support a root of trust, such as TPM or HSM, and secure boot
22	R-92207	The VNF SHOULD provide a mechanism that enables the operators to perform automated system configuration auditing at configurable time intervals.			Y	N			The platform **must** perform automated system configuration auditing at configurable time intervals.
23	R-99771	The VNF MUST have all code (e.g., QCOW2) and configuration files (e.g., HEAT template, Ansible playbook, script) hardened, or with documented recommended configurations for hardening and interfaces that allow the Operator to harden the VNF. Actions taken to harden a system include disabling all unnecessary services, and changing default values such as default credentials and community strings.							

VNF Identity and Access Management Requirements

	VNF Security Ref	Description	Notes		CNTT Relevant	Exists	CNTT Ref#	Current Description, if exists	Recommended Description (may be a modification of existing)

1	R-23135	The VNF MUST, if not integrated with the Operator's identity and access management system, authenticate all access to protected resources.							
2	R-231402	The VNF MUST provide a means to explicitly logout, thus ending that session.			Y	N			The Platform **must** provide a means to explicitly logout from an interactive session, thus ending that session. The Platform **must** provide a means to automatically logout, thus ending that session, of any interactive session after a configurable period of inactivity.
3	R-251639	The VNF MUST provide explicit confirmation of a session termination such as a message, new page, or rerouting to a login page.							
4	R-358699	The VNF MUST support at least the following roles: system administrator, application administrator, network function O&M.							
5	R-373737	The VNF MUST, if not integrated with the operator's IAM system, provide a mechanism for assigning roles and/or permissions to an identity.							
6	R-39562	The VNF MUST disable unnecessary or vulnerable cgi-bin programs.							
7	R-42874	The VNF MUST allow the Operator to restrict access to protected resources based on the assigned permissions associated with an ID in order to support Least Privilege (no more privilege than required to perform job functions).							
8	R-45719	The VNF MUST, if not integrated with the Operator's Identity and Access Management system, enforce a configurable "terminate idle sessions" policy by terminating the session after a configurable period of inactivity.							
9	R-46908	The VNF MUST, if not integrated with the Operator's Identity and Access Management system, comply with "password complexity" policy. When passwords are used, they shall be complex and shall at least meet the following password construction requirements: (1) be a minimum configurable number of characters in length, (2) include 3 of the 4 following types of characters: upper-case alphabetic, lower-case alphabetic, numeric, and special, (3) not be the same as the UserID with which they are associated or other common strings as specified by the environment, (4) not contain repeating or sequential characters or numbers, (5) not to use special characters that may have command functions, and (6) new passwords must not contain sequences of three or more characters from the previous password.			Y	N		Requirement exists in discussions but not in consolidated requirements	The Platform **must** ensure compliance with password complexity policy. When passwords are created, they shall be complex and shall at least meet the following password construction requirements: (1) be a minimum configurable number of characters in length, (2) include 3 of the 4 following types of characters: upper-case alphabetic, lower-case alphabetic, numeric, and special, (3) not be the same as the UserID with which they are associated or other common strings as specified by the environment, (4) not contain repeating or sequential characters or numbers, and (5) not be the same as a password used previously during a configurable period. The Platform **must** ensure compliance with password expiry policy. Passwords expire after a configurable period of time. Passwords expire for non-use after a configurable period of time.

10	R-479386	The VNF MUST provide the capability of setting a configurable message to be displayed after successful login. It MAY provide a list of supported character sets.							
11	R-581188	The VNF MUST NOT identify the reason for a failed authentication, only that the authentication failed.			Y	N			The Platform **must not** identify the reason for a failed authentication, only that the authentication failed. The Platform **must** limit the number of failed authentication attempts to a configurable number. When the number of failed attempts is reached, the platform **must** disable the user account; user account can be enabled by an administrator.
12	R-59391	The VNF MUST NOT allow the assumption of the permissions of another account to mask individual accountability. For example, use SUDO when a user requires elevated permissions such as root or admin.							
13	R-75041	The VNF MUST, if not integrated with the Operator's Identity and Access Management system, support configurable password expiration.							
14	R-78010	The VNF MUST support LDAP in order to integrate with an external identity and access manage system. It MAY support other identity and access management protocols.			Y	N			The Platform **must** support LDAP in order to integrate with an external identity and access manage system. It MAY support other identity and access management protocols.
15	R-79107	The VNF MUST, if not integrated with the Operator's Identity and Access Management system, support the ability to lock out the userID after a configurable number of consecutive unsuccessful authentication attempts using the same userID. The locking mechanism must be reversible by an administrator and should be reversible after a configurable time period.							
16	R-81147	The VNF MUST, if not integrated with the Operator's Identity and Access Management system, support multifactor authentication on all protected interfaces exposed by the VNF for use by human users.							
17	R-814377	The VNF MUST have the capability of allowing the Operator to create, manage, and automatically provision user accounts using one of the protocols specified in Chapter 7.							
18	R-844011	The VNF MUST not store authentication credentials to itself in clear text or any reversible form and must use salting.							
19	R-86835	The VNF MUST set the default settings for user access to deny authorization, except for a super user type of account.							
20	R-931076	The VNF MUST support account names that contain at least A-Z, a-z, and 0-9 character sets and be at least 6 characters in length.							
21	R-99174	The VNF MUST, if not integrated with the Operator's Identity and Access Management system, support the creation of multiple IDs so that individual accountability can be supported.							

VNF API Security Requirements

	VNF Security Ref	Description	Notes		CNTT Relevant	Exists	CNTT Ref#	Current Description, if exists	Recommended Description (may be a modification of existing)
1	R-21210	The VNF MUST implement the following input validation control on APIs: Validate that any input file has a correct and valid Multipurpose Internet Mail Extensions (MIME) type. Input files should be tested for spoofed MIME types.							
2	R-21652	The VNF MUST implement the following input validation control: Check the size (length) of all input. Do not permit an amount of input so great that it would cause the VNF to fail. Where the input may be a file, the VNF API must enforce a size limit.							

3	R-43884	The VNF SHOULD integrate with the Operator's authentication and authorization services (e.g., IDAM).	see also R-78010 above						
4	R-54930	The VNF MUST implement the following input validation controls: Do not permit input that contains content or characters inappropriate to the input expected by the design. Inappropriate input, such as SQL expressions, may cause the system to execute undesirable and unauthorized transactions against the database or allow other inappropriate access to the internal network (injection attacks).							

VNF Security Analytics Requirements

	VNF Security Ref	Description	Notes		CNTT Relevant	Exists	CNTT Ref#	Current Description, if exists	Recommended Description (may be a modification of existing)
1	R-04492	The VNF MUST generate security audit logs that can be sent to Security Analytics Tools for analysis.			Y	Y	7.11.7. Monitoring and Security Audit sec.mon.011 sec.mon.016	The Platform **must** Monitor and Audit logs from infrastructure elements and workloads to detected anomalies in the system components and take corrective actions accordingly The Platform Monitoring components **should** follow security best practices for auditing, including secure logging and tracing	
2	R-04982	The VNF MUST NOT include an authentication credential, e.g., password, in the security audit logs, even if encrypted.			N				
3	R-06413	The VNF MUST log the field "service or program used for access" in the security audit logs.							
4	R-07617	The VNF MUST log success and unsuccessful creation, removal, or change to the inherent privilege level of users.							
5	R-13344	The VNF MUST log starting and stopping of security logging.							
6	R-13627	The VNF MUST monitor API invocation patterns to detect anomalous access patterns that may represent fraudulent access or other types of attacks, or integrate with tools that implement anomaly and abuse detection.			Y	Y	7.11.7. Monitoring and Security Audit sec.mon.008	The Platform **must** Monitor and Audit externally exposed interfaces for illegal access (attacks) and take corrective security hardening measures	
7	R-15325	The VNF MUST log the field "success/failure" in the security audit logs.							
8	R-15884	The VNF MUST include the field "date" in the Security alarms (where applicable and technically feasible).							
9	R-22367	The VNF MUST support detection of malformed packets due to software misconfiguration or software vulnerability, and generate an error to the syslog console facility.			Y	Y	7.11.7. Monitoring and Security Audit sec.mon.009	The Platform **must** Monitor and Audit service handling for various attacks (malformed messages, signalling flooding and replaying, etc.) and take corrective actions accordingly	
10	R-23957	The VNF MUST include the field "time" in the Security alarms (where applicable and technically feasible).							
11	R-25547	The VNF MUST log the field "protocol" in the security audit logs.							
12	R-29705	The VNF MUST restrict changing the criticality level of a system security alarm to users with administrative privileges.							
13	R-303569	The VNF MUST log the Source IP address in the security audit logs.							
14	R-30932	The VNF MUST log successful and unsuccessful access to VNF resources, including data.							
15	R-31614	The VNF MUST log the field "event type" in the security audit logs.							

16	R-32636	The VNF MUST support API-based monitoring to take care of the scenarios where the control interfaces are not exposed, or are optimized and proprietary in nature.							
17	R-33488	The VNF MUST protect against all denial of service attacks, both volumetric and non-volumetric, or integrate with external denial of service protection tools.							
18	R-34552	The VNF MUST be implemented so that it is not vulnerable to OWASP Top 10 web application security risks.			Y	Y	7.11.8. Compliance with Standards sec.std. 004	The Cloud Operator, Platform and Workloads **should** ensure that their code is not vulnerable to the OWASP Top Ten Security Risks https://owasp.org/www-project-top-ten/	
19	R-41252	The VNF MUST support the capability of online storage of security audit logs.							
20	R-41825	The VNF MUST activate security alarms automatically when a configurable number of consecutive unsuccessful login attempts is reached.							
21	R-43332	The VNF MUST activate security alarms automatically when it detects the successful modification of a critical system or application file.			Y	Y	General for all monitoring requirements	2.4.8.7. Monitoring and Security Audit The Platform is assumed to provide configurable alerting and notification capability and the operator is assumed to have automated systems, policies and procedures to act on alerts and notifications in a timely fashion. In the following the monitoring and logging capabilities can trigger alerts and notifications for appropriate action.	
22	R-465236	The VNF SHOULD provide the capability of maintaining the integrity of its static files using a cryptographic method.							
23	R-48470	The VNF MUST support Real-time detection and notification of security events.							
24	R-54520	The VNF MUST log successful and unsuccessful authentication attempts, e.g., authentication associated with a transaction, authentication to create a session, authentication to assume elevated privilege.							
25	R-54816	The VNF MUST support the storage of security audit logs for a configurable period of time.							
26	R-55478	The VNF MUST log logoffs.							
27	R-56920	The VNF MUST protect all security audit logs (including API, OS and application-generated logs), security audit software, data, and associated documentation from modification, or unauthorized viewing, by standard OS access control mechanisms, by sending to a remote system, or by encryption.							
28	R-57617	The VNF MUST include the field “success/failure” in the Security alarms (where applicable and technically feasible).							
29	R-58370	The VNF SHOULD operate with anti-virus software which produces alarms every time a virus is detected.							
30	R-629534	The VNF MUST be capable of automatically synchronizing the system clock daily with the Operator’s trusted time source, to assure accurate time reporting in log files. It is recommended that Coordinated Universal Time (UTC) be used where possible, so as to eliminate ambiguity owing to daylight savings time.							
31	R-63330	The VNF MUST detect when its security audit log storage medium is approaching capacity (configurable) and issue an alarm.							
32	R-703767	The VNF MUST have the capability to securely transmit the security logs and security events to a remote system before they are purged from the system.							
33	R-71842	The VNF MUST include the field “service or program used for access” in the Security alarms (where applicable and technically feasible).							

34	R-73223	The VNF MUST support proactive monitoring to detect and report the attacks on resources so that the VNFs and associated VMs can be isolated, such as detection techniques for resource exhaustion, namely OS resource attacks, CPU attacks, consumption of kernel memory, local storage attacks.							
35	R-74958	The VNF MUST activate security alarms automatically when it detects an unsuccessful attempt to gain permissions or assume the identity of another user.							
36	R-84160	The VNF MUST have security logging for VNFs and their OSs be active from initialization. Audit logging includes automatic routines to maintain activity records and cleanup programs to ensure the integrity of the audit/logging systems.							
37	R-859208	The VNF MUST log automated remote activities performed with elevated privileges							
38	R-89474	The VNF MUST log the field “Login ID” in the security audit logs.							
39	R-94525	The VNF MUST log connections to the network listeners of the resource.							
40	R-97445	The VNF MUST log the field “date/time” in the security audit logs.							
41	R-99730	The VNF MUST include the field “Login ID” in the Security alarms (where applicable and technically feasible).							

VNF Data Protection Requirements

	VNF Security Ref	Description	Notes		CNTT Relevant	Exists	CNTT Ref#	Current Description, if exists	Recommended Description (may be a modification of existing)
1	R-02170	The VNF MUST use, whenever possible, standard implementations of security applications, protocols, and formats, e.g., S/MIME, TLS, SSH, IPSec, X.509 digital certificates for cryptographic implementations. These implementations must be purchased from reputable vendors or obtained from reputable open source communities and must not be developed in-house.							
2	R-12110	R-69610							
3	R-12467	The VNF MUST NOT use compromised encryption algorithms. For example, SHA, DSS, MD5, SHA-1 and Skipjack algorithms. Acceptable algorithms can be found in the NIST FIPS publications (https://csrc.nist.gov/publications/fips) and in the NIST Special Publications (https://csrc.nist.gov/publications/sp).							
4	R-13151	R-73067							
5	R-32641	The VNF MUST provide the capability to encrypt data on non-volatile memory.Non-volative memory is storage that is capable of retaining data without electrical power, e.g. Complementary metal-oxide-semiconductor (CMOS) or hard drives.							
6	R-47204	The VNF MUST be capable of protecting the confidentiality and integrity of data at rest and in transit from unauthorized access and modification.			Y	Y	7.11.3. Confidentiality and Integrity sec.ci.001	The Platform **must** support Confidentiality and Integrity of data at rest and in-transit	
7	R-58964	The VNF MUST provide the capability to restrict read and write access to data handled by the VNF.							
8	R-69610	The VNF MUST provide the capability of using X.509 certificates issued by an external Certificate Authority.							
9	R-70933	The VNF MUST provide the ability to migrate to newer versions of cryptographic algorithms and protocols with minimal impact.							
10	R-73067	The VNF MUST use NIST and industry standard cryptographic algorithms and standard modes of operations when implementing cryptography.							
11	R-83227	R-32641							
12	R-95864	The VNF MUST support digital certificates that comply with X.509 standards.							

VNF Cryptography Requirements

	VNF Security Ref	Description	Notes		CNTT Relevant	Exists	CNTT Ref#	Current Description, if exists	Recommended Description (may be a modification of existing)
1	R-48080	The VNF SHOULD support an automated certificate management protocol such as CMPv2, Simple Certificate Enrollment Protocol (SCEP) or Automated Certificate Management Environment (ACME).			Y	N			The Platform **should** support an automated certificate management protocol such as CMPv2, Simple Certificate Enrollment Protocol (SCEP) or Automated Certificate Management Environment (ACME).
2	R-93860	The VNF SHOULD provide the capability to integrate with an external encryption service.			Y	Y	7.11.2. Platform and Access sec.sys.012	The Platform **must** only use secrets encrypted using strong encryption techniques, and stored externally from the component (e.g., Barbican (OpenStack))	
3	R-44723	The VNF MUST use symmetric keys of at least 112 bits in length.			Y	N			The Platform **must** use symmetric keys of at least 112 bits in length.
4	R-25401	The VNF MUST use asymmetric keys of at least 2048 bits in length.			Y	N			The Platform **must** use asymmetric keys of at least 2048 bits in length.
5	R-52060	The VNF MUST provide the capability to configure encryption algorithms or devices so that they comply with the laws of the jurisdiction in which there are plans to use data encryption.			Y	N			The Platform **must** provide the capability to configure encryption algorithms or devices so that they comply with the laws of the jurisdiction in which there are plans to use data encryption.
6	R-83500	The VNF MUST provide the capability of allowing certificate renewal and revocation.			Y	N			The Platform **must** allow certificate renewal and revocation.
7	R-29977	The VNF MUST provide the capability of testing the validity of a digital certificate by validating the CA signature on the certificate.			Y	N			The Platform **must** provide the capability of testing the validity of a digital certificate by validating the CA signature on the certificate.
8	R-24359	The VNF MUST provide the capability of testing the validity of a digital certificate by validating the date the certificate is being used is within the validity period for the certificate.			Y	N			The Platform **must** provide the capability of testing the validity of a digital certificate by validating the date the certificate is being used is within the validity period for the certificate.
9	R-39604	The VNF MUST provide the capability of testing the validity of a digital certificate by checking the Certificate Revocation List (CRL) for the certificates of that type to ensure that the certificate has not been revoked.			Y	N			The Platform **must** provide the capability of testing the validity of a digital certificate by checking the Certificate Revocation List (CRL) for the certificates of that type to ensure that the certificate has not been revoked.

10	R-75343	The VNF MUST provide the capability of testing the validity of a digital certificate by recognizing the identity represented by the certificate - the “distinguished name”.			Y	N			The Platform **must** provide the capability of testing the validity of a digital certificate by recognizing the identity represented by the certificate - the “distinguished name”.
11	R-49109	The VNF or PNF MUST support HTTPS using TLS v1.2 or higher with strong cryptographic ciphers.			Y	N			see R-118669 for suggested change
12	R-41994	The VNF MUST support the use of X.509 certificates issued from any Certificate Authority (CA) that is compliant with RFC5280, e.g., a public CA such as DigiCert or Let’s Encrypt, or an RFC5280 compliant Operator CA. Note: The VNF provider cannot require the use of self-signed certificates in an Operator’ s run time environment.							