Certificado de Conformidad

Con el Esquema Nacional de Seguridad (ENS)

Número de Certificado : **ENS 844477**

British Standards Institution Group Iberia, S.A.U. (BSI Iberia) certifica que el sistema o sistemas de información evaluado(s), todos ellos de categoría ALTA, y los servicios que se relacionan, de la organización

Tanium Spain, S.L.
Avenida Diagonal, 640 - P. 6
08017 Barcelona
España

han sido auditados y encontrados conforme con las exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, según se detalla en el correspondiente Informe de Auditoría de 07/05/2026.

El Sistema de Gestión de Seguridad de la Información para la Protección de la Información del Cliente, los Datos personales de los empleados y la Propiedad Intelectual, cubriendo la infraestructura, operaciones, desarrollo y actividades de servicio, apoyando la plataforma central de Tanium, módulos de producto, soluciones y servicios en la nube, según declaración de aplicabilidad SoA ENS ALTA v1 18-03-2026.

Por y en nombre de BSI:

David Fardel, Country Manager, EMEA Assurance

Fecha inicial de certificación: 29/05/2026
Fecha de última emisión: 29/05/2026

Fecha de concesión: 29/05/2026
Fecha de expiración: 28/05/2028

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 311/2022

ENAC CERTIFICACIÓN ISO 17065 Nº252 / C-PR505

Cuadro de los niveles de seguridad auditados:

CATEGORÍA	DIMENSIONES DE SEGURIDAD					MEDIDAS
	C	I	D	A	T	Total
ALTA	Alto	Alto	Alto	Alto	Alto	*72*

Categoría de seguridad: Alta

Emitido en Madrid a 04 **de** Junio **de** 2026

Fecha inicial de certificación: 29/05/2026
Fecha de última emisión: 29/05/2026

Fecha de concesión: 29/05/2026
Fecha de expiración: 28/05/2028

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 311/2022

ENAC CERTIFICACIÓN ISO 17065 Nº252 / C-PR505

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
1	Organizational framework [org]	org.1 - Security policy		Control Objective	Approved security policy document specifying: organization objectives/mission; legal/regulatory framework; security roles/functions with duties and appointment procedures; security management committee structure; and guidelines for system security documentation.	Yes	Company	Fully Covered	
1	Organizational framework [org]	org.1 - Security policy	R1 (optional)	Reinforcement	Specific documentation as reflected in CCN-STIC guides.	No	N/A	N/A	Optional controls are not included in system scope
2	Organizational framework [org]	org.2 - Security regulations		Control Objective	Documents describing: correct use of equipment/services/facilities and what constitutes misuse; staff responsibility regarding compliance or violation of regulations including rights/duties/disciplinary measures.	Yes	Company	Fully Covered	
2	Organizational framework [org]	org.2 - Security regulations	R1	Reinforcement	Specific security documentation developed as reflected in applicable CCN-STIC guides.	Yes	Company	Fully Covered	
3	Organizational framework [org]	org.3 - Security procedures		Control Objective	Documents detailing how to operate information system elements: how to carry out usual tasks; who should do what; how to identify/report abnormal behaviors; manner of treating information per security level (access control, storage, copies, labeling, telematic transmission).	Yes	Company	Fully Covered	
3	Organizational framework [org]	org.3 - Security procedures	R1	Reinforcement	Validation of security procedures by the relevant authority.	Yes	Company	Fully Covered	
4	Organizational framework [org]	org.4 - Authorization process		Control Objective	Formal authorization process covering: use of regular/alternative facilities; incorporation of equipment/application in production; establishment of communication links; use of communication media; use of information media; use of mobile equipment; use of third-party services.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
5	Planning [op.pl]	op.pl.1 - Risk analysis		Control Objective	Informal risk analysis in natural language identifying: most valuable system assets; most likely threats; safeguards protecting against those threats; and main residual risks.	Yes	Company	Fully Covered	
5	Planning [op.pl]	op.pl.1 - Risk analysis	R1	Reinforcement	Semiformal risk analysis using specific language with a basic threat catalog (qualitative valuation of assets, quantification of threats, evaluation of safeguards and residual risk).	Yes	Company	Fully Covered	
5	Planning [op.pl]	op.pl.1 - Risk analysis	R2	Reinforcement	Formal risk analysis using internationally recognized mathematical basis (qualitative asset valuation, threat quantification, safeguard evaluation/prioritization, formal residual risk assumption).	Yes	Company	Fully Covered	
6	Planning [op.pl]	op.pl.2 - Security Architecture		Control Objective	Comprehensive security approach documenting: facilities (areas and access points); system (equipment, internal/external networks, access points); lines of defense (interconnection points, firewalls, DMZ); user identification/authentication system.	Yes	Company	Fully Covered	
6	Planning [op.pl]	op.pl.2 - Security Architecture	R1	Reinforcement	Management system relating to planning, organization and control of information security resources.	Yes	Company	Fully Covered	
6	Planning [op.pl]	op.pl.2 - Security Architecture	R2	Reinforcement	Information Security Management System regularly updated and approved.	Yes	Company	Fully Covered	
6	Planning [op.pl]	op.pl.2 - Security Architecture	R3	Reinforcement	Internal technical controls including validation of input, output and intermediate data.	Yes	Company	Fully Covered	
7	Planning [op.pl]	op.pl.3 - Acquisition of new components		Control Objective	Formal process to plan acquisition of new system components based on: risk analysis conclusions; chosen security architecture; and considering technical, training and financing needs together.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
8	Planning [op.pl]	op.pl.4 - Sizing/capacity management		Control Objective	Pre-operational study covering: processing needs; information storage needs (during processing and retention); communication needs; staffing requirements (quantity and qualification); needs for facilities and auxiliary means.	Yes	Company	Fully Covered	
8	Planning [op.pl]	op.pl.4 - Sizing/capacity management	R1	Reinforcement	Continuous improvement of capacity management with capacity forecast kept up-to-date throughout system lifecycle; tools/resources for capacity monitoring.	Yes	Company	Fully Covered	
9	Planning [op.pl]	op.pl.5 - Certified components		Control Objective	Use of CCN CPSTIC catalog for selecting security products/services forming part of the system security architecture. Products providing security services to third parties must pass qualification and be included in CPSTIC or provide compliant certification.	Yes	Company	Fully Covered	
9	Planning [op.pl]	op.pl.5 - Certified components	R1	Reinforcement	Protection against TEMPEST electromagnetic emission threats per applicable regulations.	Yes	Subprocessor	Fully Covered	
9	Planning [op.pl]	op.pl.5 - Certified components	R2	Reinforcement	Each product/service shall include a list of software components as specified in [mp.sw.1.r5].	Yes	Company	Fully Covered	
10	Access control [op.acc]	op.acc.1 - Identification		Control Objective	Unique identification of system users: using identification systems per applicable regulation; separate unique identifiers per role; each entity accessing the system has a unique identifier; account management (association, disabling, retention).	Yes	Company	Fully Covered	
10	Access control [op.acc]	op.acc.1 - Identification	R1	Reinforcement	Advanced Identification -- identification allows singling out the person and their responsibilities; identification data used to determine user privileges; updated list of authorized users maintained by system administrator.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
11	Access control [op.acc]	op.acc.2 - Access requirements		Control Objective	System resources protected by mechanisms preventing use except by entities with sufficient access rights; access rights set by resource owner per security policy; controlled access to operating system components and configuration files.	Yes	Company	Fully Covered	
11	Access control [op.acc]	op.acc.2 - Access requirements	R1	Reinforcement	Access privileges -- all authorized users have individually maintained security attributes (privileges); access privileges restrict type of access (read, write, modify, delete).	Yes	Company	Fully Covered	
11	Access control [op.acc]	op.acc.2 - Access requirements	R2 (optional)	Reinforcement	Solutions for establishing device access controls per organization security policy.	No	N/A	N/A	Optional controls are not included in system scope
12	Access control [op.acc]	op.acc.3 - Segregation of functions and tasks		Control Objective	Access control organized to require two or more persons for critical tasks; development and operational capabilities should not lie with the same person; authorizers and controllers of use should be different.	Yes	Company	Fully Covered	
12	Access control [op.acc]	op.acc.3 - Segregation of functions and tasks	R1	Reinforcement	Strict Segregation -- same person should not combine system configuration and maintenance functions; same person should not combine audit/oversight with any other function.	Yes	Company	Fully Covered	
12	Access control [op.acc]	op.acc.3 - Segregation of functions and tasks	R2 (optional)	Reinforcement	Accounts with strictly controlled and personalized audit privileges.	No	N/A	N/A	Optional controls are not included in system scope
12	Access control [op.acc]	op.acc.3 - Segregation of functions and tasks	R3 (optional)	Reinforcement	Access to system security information allowed only to authorized administrators.	No	N/A	N/A	Optional controls are not included in system scope
13	Access control [op.acc]	op.acc.4 - Access rights management process		Control Objective	Access rights limited by: all access prohibited unless expressly authorized; minimum privilege principle; need-to-know and responsibility-to-share; capability to authorize (access authorization only by authorized personnel with regular review); specific remote access policy.	Yes	Company	Fully Covered	
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)		Control Objective	Authentication of non-organization users: reliable identification/registration before credentials; user acknowledgment of obligations; credentials under sole user control; credential change intervals; disabling on loss/suspicion/relationship end; minimal system info disclosure; limited login attempts; user rights notification.	Yes	Company	Fully Covered	
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)	R1	Reinforcement	Passwords with minimal complexity/robustness standards.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)	R2	Reinforcement	Password + OTP (one-time password).	Yes	Company	Fully Covered	
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)	R3	Reinforcement	Qualified certificates with second factor (PIN/biometric) and prior in-person/telematic registration.	No	N/A	N/A	Qualified certificate authentication is not implemented. External users authenticate using username/password within MFA.
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)	R4	Reinforcement	Qualified certificates on physical device (card) using CCN-authorized algorithms with second factor.	No	N/A	N/A	Qualified certificate authentication on physical devices is notimplemented;system authentication relieson MFA-based credentials.
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)	R5	Reinforcement	Registration -- record of successful/failed accesses; user informed of last access.	Yes	Company	Fully Covered	
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)	R6 (optional)	Reinforcement	Limitation of access window -- renewal of authentication required.	No	N/A	N/A	Optional controls are not included in system scope
14	Access control [op.acc]	op.acc.5 - Authentication mechanism (external users)	R7 (optional)	Reinforcement	Suspension of credentials after period of non-use.	No	N/A	N/A	Optional controls are not included in system scope
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)		Control Objective	Authentication of organization staff (own or contracted): knowledge/acceptance of security policy before credentials; user acknowledgment of credential custody obligations; credentials under sole user control; change intervals; disabling on loss/suspicion/relationship end; minimal info disclosure; limited login attempts; user rights notification.	Yes	Company	Fully Covered	
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R1	Reinforcement	Passwords with minimal complexity/robustness standards from controlled areas.	Yes	Company	Fully Covered	
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R2	Reinforcement	Password + second factor (device, OTP, or biometric).	Yes	Company	Fully Covered	

ENS Statement of Applicability
Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R3	Reinforcement	Qualified certificates with second factor (PIN/biometric).	No	N/A	N/A	Qualified certificate authentication on physical devices is notimplemented;system authentication relieson MFA-based credentials.
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R4	Reinforcement	Qualified certificates on physical device using CCN-authorized algorithms with second factor.	No	N/A	N/A	Qualified certificate authentication on physical devices is notimplemented;system authentication relieson MFA-based credentials.
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R5	Reinforcement	Registration -- record of successful/failed accesses; user informed of last access.	Yes	Company	Fully Covered	
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R6	Reinforcement	Limitation of access window -- session renewal points defined.	No	Company	N/A	Optional control not included in system scope.
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R7	Reinforcement	Suspension of credentials after defined period of non-use.	Yes	Company	Fully Covered	
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R8	Reinforcement	Double factor required for access from/through uncontrolled areas (R2, R3 or R4).	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
15	Access control [op.acc]	op.acc.6 - Authentication mechanism (organization users)	R9	Reinforcement	Remote access -- STI interconnection applies; authorization, encrypted traffic, disable when not in constant use, audit records.	Yes	Company	Fully Covered	
16	Operation [op.exp]	op.exp.1 - Asset inventory		Control Objective	Maintain an updated inventory of all system elements, detailing their nature and identifying their controller (person who makes decisions regarding it).	Yes	Company	Fully Covered	
16	Operation [op.exp]	op.exp.1 - Asset inventory	R1 (optional)	Reinforcement	Tagging Inventory -- labelling of equipment and wiring.	No	N/A	N/A	Optional controls are not included in system scope
16	Operation [op.exp]	op.exp.1 - Asset inventory	R2 (optional)	Reinforcement	Periodic asset identification -- tools for continuous display of status of all network computers.	No	N/A	N/A	Optional controls are not included in system scope
16	Operation [op.exp]	op.exp.1 - Asset inventory	R3 (optional)	Reinforcement	Identification of critical assets by organization context and security risks.	No	N/A	N/A	Optional controls are not included in system scope
16	Operation [op.exp]	op.exp.1 - Asset inventory	R4 (optional)	Reinforcement	List of software components -- formal list of third-party software components used in system deployment.	No	N/A	N/A	Optional controls are not included in system scope
17	Operation [op.exp]	op.exp.2 - Security Configuration		Control Objective	Computers configured prior to entry into operation: standard accounts/passwords removed; minimum functionality rule applied; default security rule applied (respectful/protective to user); virtual machines configured/managed securely including patching and antivirus.	Yes	Company	Fully Covered	
18	Operation [op.exp]	op.exp.3 - Security Configuration Management		Control Objective	Continuous management of system component configuration ensuring: minimum function rule maintained; minimum privilege rule maintained; system adapted to new authorized needs; system reacts to reported vulnerabilities; system reacts to incidents; security settings editable only by authorized personnel.	Yes	Company	Fully Covered	
18	Operation [op.exp]	op.exp.3 - Security Configuration Management	R1	Reinforcement	Regular maintenance -- authorized and regularly maintained hardware/software configurations; periodic checks for unauthorized elements; list of authorized services.	Yes	Company	Fully Covered	
18	Operation [op.exp]	op.exp.3 - Security Configuration Management	R2	Reinforcement	Responsibility -- security configuration of OS/applications is responsibility of very limited number of administrators.	Yes	Company	Fully Covered	
18	Operation [op.exp]	op.exp.3 - Security Configuration Management	R3	Reinforcement	Security backups of system configuration for rebuild after incident.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
18	Operation [op.exp]	op.exp.3 - Security Configuration Management	R4 (optional)	Reinforcement	Application of configuration through manual/automated installation of version modifications and security updates.	No	N/A	N/A	Optional controls are not included in system scope
18	Operation [op.exp]	op.exp.3 - Security Configuration Management	R5 (optional)	Reinforcement	Tools for knowing security status of network device configuration.	No	N/A	N/A	Optional controls are not included in system scope
19	Operation [op.exp]	op.exp.4 - Security maintenance and updates		Control Objective	Maintain physical and logical equipment: meet manufacturer specifications; procedure to analyze/prioritize/apply security updates, patches, upgrades considering risk; maintenance only by authorized personnel.	Yes	Company	Fully Covered	
19	Operation [op.exp]	op.exp.4 - Security maintenance and updates	R1	Reinforcement	Tests in pre-production -- new/patched versions tested in controlled environment before production.	Yes	Company	Fully Covered	
19	Operation [op.exp]	op.exp.4 - Security maintenance and updates	R2	Reinforcement	Failure prevention -- mechanism to reverse updates in event of adverse effects.	Yes	Company	Fully Covered	
19	Operation [op.exp]	op.exp.4 - Security maintenance and updates	R3 (optional)	Reinforcement	Updates and periodic tests -- periodic integrity check of firmware (BIOS, network infrastructure).	No	N/A	N/A	Optional controls are not included in system scope
19	Operation [op.exp]	op.exp.4 - Security maintenance and updates	R4 (optional)	Reinforcement	Continuous monitoring strategy for threats/vulnerabilities with critical security indicators and patch application policy.	No	N/A	N/A	Optional controls are not included in system scope
20	Operation [op.exp]	op.exp.5 - Change Management		Control Objective	Continuous monitoring of system changes: planned changes to reduce impact; recorded change requests with reference numbers; pre-production tests; risk analysis for security relevance (HIGH risk changes require security officer approval); acceptance tests and documentation updates after implementation.	Yes	Company	Fully Covered	
20	Operation [op.exp]	op.exp.5 - Change Management	R1	Reinforcement	Prevention of failures -- possibility to reverse changes in event of adverse effects; all hardware/software failures communicated to security officer; all changes documented with security impact assessment.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
21	Operation [op.exp]	op.exp.6 - Protection against harmful code		Control Objective	Preventive and reaction mechanisms against harmful code per manufacturer recommendations; harmful code protection software on all equipment (workstations, servers, perimeter); external files analyzed before use; detection databases permanently updated; real-time protection on workstations.	Yes	Company	Fully Covered	
21	Operation [op.exp]	op.exp.6 - Protection against harmful code	R1	Reinforcement	Periodic scanning -- entire system scanned regularly.	Yes	Company	Fully Covered	
21	Operation [op.exp]	op.exp.6 - Protection against harmful code	R2	Reinforcement	Preventive system review -- critical functions analyzed at boot for unauthorized modifications.	Yes	Company	Fully Covered	
21	Operation [op.exp]	op.exp.6 - Protection against harmful code	R3	Reinforcement	Whitelist -- only previously authorized applications may execute.	Yes	Company	Fully Covered	
21	Operation [op.exp]	op.exp.6 - Protection against harmful code	R4	Reinforcement	EDR (Endpoint Detection and Response) -- tools for detecting, investigating and resolving suspicious activities.	Yes	Company	Fully Covered	
21	Operation [op.exp]	op.exp.6 - Protection against harmful code	R5 (optional)	Reinforcement	Advanced configuration of detection tool including boot review and removable device scanning; real-time protection on servers and perimeter elements.	No	N/A	N/A	Optional controls are not included in system scope
22	Operation [op.exp]	op.exp.7 - Incident management		Control Objective	Comprehensive incident management process: report of security events/weaknesses with classification criteria and escalation; management of personal data incidents per GDPR/national law.	Yes	Company	Fully Covered	
22	Operation [op.exp]	op.exp.7 - Incident management	R1	Reinforcement	Notification -- one-stop-shop solutions for reporting incidents to CCN-CERT in federated manner.	Yes	Company	Fully Covered	
22	Operation [op.exp]	op.exp.7 - Incident management	R2	Reinforcement	Detection and Response -- urgent measures (service detention, isolation, evidence collection); resources for investigation; inform information/service managers; measures to prevent recurrence and update procedures.	Yes	Company	Fully Covered	
22	Operation [op.exp]	op.exp.7 - Incident management	R3	Reinforcement	Dynamic Reconfiguration -- changes to router rules, ACLs, IDS/IPS parameters, firewall rules, critical element isolation; adapt to CCN-CERT announcements on advanced threats.	Yes	Company	Fully Covered	
22	Operation [op.exp]	op.exp.7 - Incident management	R4 (optional)	Reinforcement	Prevention and automatic response tools for anomaly detection, dynamic network segmentation, critical device isolation.	No	N/A	N/A	Optional controls are not included in system scope

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
23	Operation [op.exp]	op.exp.8 - Recording of the activity		Control Objective	Audit log generation including: user/entity identifier, date/time, target information, event type, outcome (success/failure); activity recording activated on servers.	Yes	Company	Fully Covered	
23	Operation [op.exp]	op.exp.8 - Recording of the activity	R1	Reinforcement	Review of records -- regular informal review looking for abnormal patterns.	Yes	Company	Fully Covered	
23	Operation [op.exp]	op.exp.8 - Recording of the activity	R2	Reinforcement	Clock synchronization -- time reference (timestamp) with administration-controlled modification and integrity/authentication mechanisms.	Yes	Company	Fully Covered	
23	Operation [op.exp]	op.exp.8 - Recording of the activity	R3	Reinforcement	Retention of records -- documented auditable security events and retention time.	Yes	Company	Fully Covered	
23	Operation [op.exp]	op.exp.8 - Recording of the activity	R4	Reinforcement	Access control -- activity records and backups accessible/deletable only by authorized personnel.	Yes	Company	Fully Covered	
23	Operation [op.exp]	op.exp.8 - Recording of the activity	R5	Reinforcement	Automatic review and correlation -- tools for analysis of system activity and audit information; automatic collection/correlation/response system.	Yes	Company	Fully Covered	
24	Operation [op.exp]	op.exp.9 - Incident management record		Control Objective	Record of all incident management actions: initial/intermediate/final reports, emergency actions, system modifications; evidence recorded for potential jurisdictional proceedings (disciplinary/criminal) with legal advice; review of auditable events determination.	Yes	Company	Fully Covered	
25	Operation [op.exp]	op.exp.10 - Cryptographic Key Protection		Control Objective	Protection of crypto keys throughout lifecycle: generation, transport to point of operation, safekeeping during operation, archive after decommissioning, final destruction. Generation means isolated from exploitation means; archived keys isolated from exploitation.	Yes	Company	Fully Covered	
25	Operation [op.exp]	op.exp.10 - Cryptographic Key Protection	R1	Reinforcement	Algorithms and parameters authorized by the CCN.	Yes	Company	Fully Covered	
25	Operation [op.exp]	op.exp.10 - Cryptographic Key Protection	R2 (optional)	Reinforcement	Advanced cryptographic key protection using encryptors meeting applicable CCN-STIC guide requirements.	No	N/A	N/A	Optional controls are not included in system scope

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
26	[op.ext]	service level agreements		Control Objective	provider; consequences of breaches.	Yes	Company	Fully Covered	
27	External resources [op.ext]	op.ext.2 - Daily management		Control Objective	Routine system for measuring compliance with service obligations including procedure for neutralizing deviations outside agreed tolerance; coordination mechanism and procedures for maintenance of systems covered by agreement including incidents and disasters.	Yes	Company	Fully Covered	
28	External resources [op.ext]	op.ext.3 - Protection of the supply chain		Control Objective	Analysis of impact of accidental or deliberate incident originating in supply chain on the system; estimation of risk due to estimated impact; measures to contain estimated impacts.	Yes	Company	Fully Covered	
28	External resources [op.ext]	op.ext.3 - Protection of the supply chain	R1 (optional)	Reinforcement	Contingency plan -- organizational continuity plan considers dependency on critical external suppliers; continuity tests include supplier failure scenarios.	No	N/A	N/A	Optional controls are not included in system scope
28	External resources [op.ext]	op.ext.3 - Protection of the supply chain	R2 (optional)	Reinforcement	Security management system -- protection of processes and information flows in online supply chain relationships.	No	N/A	N/A	Optional controls are not included in system scope
28	External resources [op.ext]	op.ext.3 - Protection of the supply chain	R3 (optional)	Reinforcement	List of software components -- formal record of supply chain component details per [mp.sw.1.r5].	No	N/A	N/A	Optional controls are not included in system scope
29	External resources [op.ext]	op.ext.4 - Interconnection of systems		Control Objective	All information exchanges and service provision with other systems subject to prior authorization; prohibited flows unless expressly authorized; each interconnection documented (interface characteristics, security/data protection requirements, nature of information exchanged).	Yes	Company	Fully Covered	
29	External resources [op.ext]	op.ext.4 - Interconnection of systems	R1	Reinforcement	Coordination of activities -- when systems interconnect across different security domains with different responsibilities, local security measures accompanied by coordination mechanisms and procedures for effective attribution of responsibilities.	Yes	Company	Fully Covered	
30	Cloud Services [op.nub]	op.nub.1 - Cloud Service Protection		Control Objective	Cloud service systems for public sector must comply with security measures by service model (SaaS, PaaS, IaaS) per CCN-STIC guides. Third-party cloud services must comply with ENS or CCN-STIC guide requirements covering: penetration tests, transparency, encryption/key management, data jurisdiction.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
30	Cloud Services [op.nub]	op.nub.1 - Cloud Service Protection	R2	Reinforcement	Specific Security Configuration Guides -- security configuration per relevant CCN-STIC Guide for both user and provider.	Yes	Company	Fully Covered	
31	Continuity of service [op.cont]	op.cont.1 - Impact analysis		Control Objective	Impact analysis to determine availability requirements for each service (impact of interruption over given period), and identify elements critical to provision of each service.	Yes	Company	Fully Covered	
32	Continuity of service [op.cont]	op.cont.2 - Continuity plan		Control Objective	Continuity plan covering: identified functions/responsibilities/activities; provision for coordination of alternative means entry into service; all alternative means planned/materialized in agreements; specific training for affected persons; plan integrated with organization's continuity plans.	Yes	Company	Fully Covered	
32	Continuity of service [op.cont]	op.cont.2 - Continuity plan	R1 (optional)	Reinforcement	Emergency and contingency plan where continuity needs identified.	No	N/A	N/A	Optional controls are not included in system scope
32	Continuity of service [op.cont]	op.cont.2 - Continuity plan	R2 (optional)	Reinforcement	Integrity check of operating system, firmware and configuration files in event of failure or discontinuity.	No	N/A	N/A	Optional controls are not included in system scope
33	Continuity of service [op.cont]	op.cont.3 - Periodic tests		Control Objective	Periodic tests to identify and correct errors or deficiencies in the continuity plan.	Yes	Company	Fully Covered	
34	Continuity of service [op.cont]	op.cont.4 - Alternative means		Control Objective	Provision for availability of alternative means when usual means unavailable, covering: third-party services, alternative facilities, staff, computer equipment, and media. Maximum time set for alternative means to become operational; subject to same security guarantees as originals.	Yes	Company	Fully Covered	
34	Continuity of service [op.cont]	op.cont.4 - Alternative means	R1 (optional)	Reinforcement	Automation of transition -- hardware/software elements for automatic transfer of services to alternative media.	No	N/A	N/A	Optional controls are not included in system scope
35	System monitoring [op.mon]	op.mon.1 - Intrusion detection		Control Objective	Intrusion detection or prevention tools shall be available.	Yes	Company	Fully Covered	
35	System monitoring [op.mon]	op.mon.1 - Intrusion detection	R1	Reinforcement	Detection based on rules -- rules-based intrusion detection or prevention tools.	Yes	Company	Fully Covered	
35	System monitoring [op.mon]	op.mon.1 - Intrusion detection	R2	Reinforcement	Response procedures -- procedures for responding to alerts generated by the IDS/IPS.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
35	System monitoring [op.mon]	op.mon.1 - Intrusion detection	R3 (optional)	Reinforcement	Default actions -- automatic execution of default actions (ending process, disabling services, disconnecting users, blocking accounts).	No	N/A	N/A	Optional controls are not included in system scope
36	System monitoring [op.mon]	op.mon.2 - Metrics system		Control Objective	Collection of necessary data to determine degree of implementation of applicable security measures and provide annual report per Article 32.	Yes	Company	Fully Covered	
36	System monitoring [op.mon]	op.mon.2 - Metrics system	R1	Reinforcement	Effectiveness of incident management system -- accurate data on incident management behavior per TSI for Security Incident Notification.	Yes	Company	Fully Covered	
36	System monitoring [op.mon]	op.mon.2 - Metrics system	R2	Reinforcement	Efficiency of security management system -- data on efficiency relative to resources consumed (hours and budget).	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring		Control Objective	Automatic security event collection system.	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring	R1	Reinforcement	Correlation of events -- automatic collection system allowing event correlation.	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring	R2	Reinforcement	Dynamic analysis -- monitoring solutions to determine exposure area in relation to vulnerabilities and configuration deficiencies.	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring	R3	Reinforcement	Advanced Cyber Threats -- systems for detection of advanced threats and abnormal behavior; APT detection via network traffic anomalies.	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring	R4	Reinforcement	Digital Observatories -- cyber-monitoring for detecting/tracking anomalies representing threat indicators.	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring	R5	Reinforcement	Data Mining -- limitation of queries (monitoring volume/frequency); real-time alerts to administrators of suspicious behaviors.	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring	R6	Reinforcement	Security Inspections -- periodic configuration checks, vulnerability analysis, penetration tests.	Yes	Company	Fully Covered	
37	System monitoring [op.mon]	op.mon.3 - Monitoring	R7 (optional)	Reinforcement	Interconnections -- controls on information exchange flows through metadata.	No	N/A	N/A	Optional controls are not included in system scope

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
38	Protection of facilities [mp.if]	mp.if.1 - Separate areas with access control		Control Objective	Data Processing Centre equipment installed in separate areas specific to its function, as far as possible; access controlled so that only intended entries are used.	Yes	Subprocessor	Fully Covered	
39	Protection of facilities [mp.if]	mp.if.2 - Identification of persons		Control Objective	Access control procedure identifies persons accessing premises where essential DPC information system equipment is located, recording corresponding inputs and exits.	Yes	Subprocessor	Fully Covered	
40	Protection of facilities [mp.if]	mp.if.3 - Fitting-out of premises		Control Objective	Premises equipped with appropriate elements for efficient operation: temperature and humidity conditions; protection from threats identified in risk analysis; protection of wiring against accidental or deliberate incidents.	Yes	Subprocessor	Fully Covered	
41	Protection of facilities [mp.if]	mp.if.4 - Electrical energy		Control Objective	Premises with electrical power outlets ensuring supply and proper operation of emergency lights.	Yes	Subprocessor	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
41	Protection of facilities [mp.if]	mp.if.4 - Electrical energy	R1	Reinforcement	Emergency Electrical Supply -- power supply guaranteed for sufficient time for orderly completion of processes and information safeguarding in event of main supply failure.	Yes	Subprocessor	Fully Covered	
42	Protection of facilities [mp.if]	mp.if.5 - Fire protection		Control Objective	Premises protected against fires in accordance with at least applicable industrial regulations.	Yes	Subprocessor	Fully Covered	
43	Protection of facilities [mp.if]	mp.if.6 - Flood protection		Control Objective	Facilities where information systems and essential components are located protected against water incidents.	Yes	Subprocessor	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
44	Protection of facilities [mp.if]	mp.if.7 - Recording of entries and exits of equipment		Control Objective	Detailed record of any entry and exit of essential equipment, including identification of the person authorizing the movement.	Yes	Subprocessor	Fully Covered	
45	Staff management [mp.per]	mp.per.1 - Job characterization		Control Objective	For each job related to handling information/services: security responsibilities defined based on risk analysis; requirements for persons to be employed defined (particularly confidentiality), considered in selection including history/training/references verification.	Yes	Company	Fully Covered	
45	Staff management [mp.per]	mp.per.1 - Job characterization	R1 (optional)	Reinforcement	Personal Security Clearance (PSC) -- security/system administrators shall have PSC granted by competent authority as consequence of risk analysis.	No	N/A	N/A	Optional controls are not included in system scope
46	Staff management [mp.per]	mp.per.2 - Duties and obligations		Control Objective	Each person informed of duties/responsibilities in security matters: disciplinary measures; obligations during assignment and upon termination/transfer; duty of confidentiality (during assignment and after termination); for third-party personnel: duties/obligations of each party established; procedure for resolving non-compliance incidents.	Yes	Company	Fully Covered	
46	Staff management [mp.per]	mp.per.2 - Duties and obligations	R1	Reinforcement	Express confirmation -- express confirmation obtained that users are aware of and accept mandatory security instructions and procedures.	Yes	Company	Fully Covered	
47	Staff management [mp.per]	mp.per.3 - Awareness		Control Objective	Regular awareness actions about role/responsibility so security reaches required standards: security regulations for proper use of common equipment/systems and social engineering; identification of suspicious incidents/activities/behaviors to report; procedure for reporting security incidents.	Yes	Company	Fully Covered	
48	Staff management [mp.per]	mp.per.4 - Training		Control Objective	Regular training on information security matters: configuration of systems; detection and response to incidents; information management in any medium (storage, transfer, copying, distribution, destruction). Effectiveness of training actions assessed.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
49	Protection of equipment [mp.eq]	mp.eq.1 - Clear desk		Control Objective	Workplaces remain clear without any material other than that required at all times.	Yes	Subprocessor	Fully Covered	
49	Protection of equipment [mp.eq]	mp.eq.1 - Clear desk	R1	Reinforcement	Storage material -- once used and whenever feasible, material stored in a closed place.	Yes	Subprocessor	Fully Covered	
50	Protection of equipment [mp.eq]	mp.eq.2 - User session lockout		Control Objective	User session locked after reasonable period of inactivity, requiring new authentication to resume activity.	Yes	Company	Fully Covered	
50	Protection of equipment [mp.eq]	mp.eq.2 - User session lockout	R1	Reinforcement	Closing of sessions -- after a certain period longer than lockout period, sessions opened from the workstation are cancelled. CCN-STIC Guide specifies security configuration adapted to system categorization.	Yes	Company	Fully Covered	
51	Protection of equipment [mp.eq]	mp.eq.3 - Protection of portable devices		Control Objective	Protection of equipment likely to leave organization premises (laptops, tablets): portable device inventory with responsible person and regular checks; security procedure for loss/theft reporting; remote connection scope limited to minimum required services; portable device prevented from containing unnecessary remote access keys.	Yes	Company	Fully Covered	
51	Protection of equipment [mp.eq]	mp.eq.3 - Protection of portable devices	R1	Reinforcement	Encryption of disc -- hard drive encrypted when confidentiality level is MEDIUM.	Yes	Company	Fully Covered	
51	Protection of equipment [mp.eq]	mp.eq.3 - Protection of portable devices	R2	Reinforcement	Protected environments -- use outside organization restricted to controlled environments safe from theft and prying eyes.	Yes	Company	Fully Covered	
52	Protection of equipment [mp.eq]	mp.eq.4 - Other devices connected to the network		Control Objective	Security configuration for devices connected to network (multifunctional, multimedia, IoT, BYOD): appropriate security configuration ensuring control of defined information flows; devices with storage must provide functionality to remove information from media.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
52	Protection of equipment [mp.eq]	mp.eq.4 - Other devices connected to the network	R1	Reinforcement	Certified products -- products or services complying with [op.pl.5] shall be used where possible.	Yes	Subprocessor	Fully Covered	
52	Protection of equipment [mp.eq]	mp.eq.4 - Other devices connected to the network	R2 (optional)	Reinforcement	Solutions for visualizing devices on network, controlling connection/disconnection, and verifying security settings.	No	N/A	N/A	Optional controls are not included in system scope
53	Protection of communications [mp.com]	mp.com.1 - Secure perimeter		Control Objective	Perimeter protection system separating internal network from outside; all traffic must pass through it; all information flows across perimeter must be pre-authorized. TSI for Interconnection determines perimeter requirements by category.	Yes	Company	Fully Covered	
54	Protection of communications [mp.com]	mp.com.2 - Protection of confidentiality		Control Objective	Encrypted virtual private networks used when communication takes place over networks outside the security domain.	Yes	Company	Fully Covered	
54	Protection of communications [mp.com]	mp.com.2 - Protection of confidentiality	R1	Reinforcement	Algorithms and parameters authorized by the CCN.	Yes	Subprocessor	Fully Covered	
54	Protection of communications [mp.com]	mp.com.2 - Protection of confidentiality	R2	Reinforcement	Hardware devices used in establishment and use of the VPN.	Yes	Subprocessor	Fully Covered	
54	Protection of communications [mp.com]	mp.com.2 - Protection of confidentiality	R3	Reinforcement	Certified products or services complying with [op.pl.5].	Yes	Subprocessor	Fully Covered	
54	Protection of communications [mp.com]	mp.com.2 - Protection of confidentiality	R4 (optional)	Reinforcement	Encryptors meeting applicable CCN-STIC guide requirements.	No	N/A	N/A	Optional controls are not included in system scope
54	Protection of communications [mp.com]	mp.com.2 - Protection of confidentiality	R5 (optional)	Reinforcement	All transmitted information encrypted.	No	N/A	N/A	Optional controls are not included in system scope

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
55	Protection of communications [mp.com]	mp.com.3 - Protection of integrity and authenticity		Control Objective	Authenticity of other end ensured before exchanging information with points outside own security domain; active attacks prevented (alteration of data in transit, injection of spurious information, session hijacking); any legally provided identification/authentication mechanism accepted.	Yes	Company	Fully Covered	
55	Protection of communications [mp.com]	mp.com.3 - Protection of integrity and authenticity	R1	Reinforcement	Encrypted VPNs when communicating over networks outside security domain.	Yes	Company	Fully Covered	
55	Protection of communications [mp.com]	mp.com.3 - Protection of integrity and authenticity	R2	Reinforcement	Algorithms and parameters authorized by the CCN.	Yes	Subprocessor	Fully Covered	
55	Protection of communications [mp.com]	mp.com.3 - Protection of integrity and authenticity	R3	Reinforcement	Hardware devices recommended for VPN.	Yes	Subprocessor	Fully Covered	
55	Protection of communications [mp.com]	mp.com.3 - Protection of integrity and authenticity	R4	Reinforcement	Certified products per [op.pl.5].	Yes	Company	Fully Covered	
55	Protection of communications [mp.com]	mp.com.3 - Protection of integrity and authenticity	R5 (optional)	Reinforcement	Encryptors meeting CCN-STIC guide requirements.	No	N/A	N/A	Optional controls are not included in system scope
56	Protection of communications [mp.com]	mp.com.4 - Separation of information flows on the network		Control Objective	Information flows separated into segments: network traffic segregated so each computer only accesses needed information; wireless communications in separate segment.	Yes	Company	Fully Covered	
56	Protection of communications [mp.com]	mp.com.4 - Separation of information flows on the network	R1	Reinforcement	Basic Logic Segmentation -- VLANs with segregation into at least users/services/administration subnets.	Yes	Company	Fully Covered	
56	Protection of communications [mp.com]	mp.com.4 - Separation of information flows on the network	R2	Reinforcement	Advanced Logic Segmentation -- VPN-based network segments.	Yes	Company	Fully Covered	
56	Protection of communications [mp.com]	mp.com.4 - Separation of information flows on the network	R3	Reinforcement	Physical segmentation -- separate physical means.	Yes	Company	Fully Covered	
56	Protection of communications [mp.com]	mp.com.4 - Separation of information flows on the network	R4	Reinforcement	Interconnection points -- user input control per segment; information input/output control; interconnection point specially secured, maintained and monitored.	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
57	Protection of information media [mp.si]	mp.si.1 - Marking		Control Objective	Information media (printed paper, electronic documents, multimedia) containing information requiring specific security measures shall bear markings or metadata indicating the level of security of the highest-rated information contained.	Yes	Company	Fully Covered	
57	Protection of information media [mp.si]	mp.si.1 - Marking	R1 (optional)	Reinforcement	Digital Watermark -- watermarks defined per security policy; digital media may include watermark; computers/devices display on-screen watermark.	No	N/A	N/A	Optional controls are not included in system scope
58	Protection of information media [mp.si]	mp.si.2 - Cryptography		Control Objective	Cryptographic mechanisms to ensure confidentiality and integrity of information contained (particularly removable devices leaving controlled areas); algorithms and parameters authorized by the CCN.	Yes	Company	Fully Covered	
58	Protection of information media [mp.si]	mp.si.2 - Cryptography	R1	Reinforcement	Certified products per [op.pl.5].	Yes	Subprocessor	Fully Covered	
58	Protection of information media [mp.si]	mp.si.2 - Cryptography	R2	Reinforcement	Security backups encrypted using CCN-authorized algorithms and parameters.	Yes	Company	Fully Covered	
59	Protection of information media [mp.si]	mp.si.3 - Custody		Control Objective	Due diligence and control applied to information media under organization responsibility, ensuring access control with physical measures ([mp.if.1] and [mp.if.7]) or logic ([mp.si.2]); manufacturer maintenance requirements respected (temperature, humidity, environmental agents).	Yes	Company	Fully Covered	
60	Protection of information media [mp.si]	mp.si.4 - Transport		Control Objective	Devices protected during movement outside controlled areas: entry/exit record identifying carrier; routine procedure to cross-check departures with arrivals and raise alarms; cryptographic protection per [mp.si.2] corresponding to highest security level; keys managed per [op.exp.10].	Yes	Subprocessor	Fully Covered	
61	Protection of information media [mp.si]	mp.si.5 - Erasure and Destruction		Control Objective	allow secure deletion, support may not be reused. CCN-STIC guides specify criteria for safe deletion/destruction mechanisms.	Yes	Subprocessor	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
61	Protection of information media [mp.si]	mp.si.5 - Erasure and Destruction	R1	Reinforcement	Certified products or services per [op.pl.5].	Yes	Subprocessor	Fully Covered	
61	Protection of information media [mp.si]	mp.si.5 - Erasure and Destruction	R2 (optional)	Reinforcement	Destruction of supports -- safe destruction upon completion of information support lifecycle per CCN criteria.	No	N/A	N/A	Optional controls are not included in system scope
62	Protection of IT applications [mp.sw]	mp.sw.1 - IT Applications development		Control Objective	Application development on separate/isolated system from production (no dev tools or data in production, no production data in development).	Yes	Company	Fully Covered	
62	Protection of IT applications [mp.sw]	mp.sw.1 - IT Applications development	R1	Reinforcement	Minimum privilege -- applications developed accessing only essential resources with indispensable privileges.	Yes	Company	Fully Covered	
62	Protection of IT applications [mp.sw]	mp.sw.1 - IT Applications development	R2	Reinforcement	Safe Development Methodology -- recognized methodology considering security aspects throughout lifecycle; secure programming rules (memory management, overflow); specific test data processing; source code inspection.	Yes	Company	Fully Covered	
62	Protection of IT applications [mp.sw]	mp.sw.1 - IT Applications development	R3	Reinforcement	Security from design -- identification/authentication mechanisms, information protection mechanisms, and audit trail generation/treatment as integral system design elements.	Yes	Company	Fully Covered	
62	Protection of IT applications [mp.sw]	mp.sw.1 - IT Applications development	R4	Reinforcement	Test data -- preferably no actual data in pre-deployment tests; if necessary, corresponding security level ensured.	Yes	Company	Fully Covered	
62	Protection of IT applications [mp.sw]	mp.sw.1 - IT Applications development	R5 (optional)	Reinforcement	List of software components -- developer maintains formal list of third-party software components with version history.	No	N/A	N/A	Optional controls are not included in system scope
63	Protection of IT applications [mp.sw]	mp.sw.2 - Acceptance and commissioning		Control Objective	Verification of correct application operation before production: security acceptance criteria met; security of other service components not impaired.	Yes	Company	Fully Covered	
63	Protection of IT applications [mp.sw]	mp.sw.2 - Acceptance and commissioning	R1	Reinforcement	Tests in isolated pre-production environment.	Yes	Company	Fully Covered	
63	Protection of IT applications [mp.sw]	mp.sw.2 - Acceptance and commissioning	R2 (optional)	Reinforcement	Inspection of source code -- source code audit.	No	N/A	N/A	Optional controls are not included in system scope

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
64	information [mp.info]	mp.info.1 - Personal data		Control Objective	rights/freedoms per GDPR Articles 24 and 32, and data protection impact assessment if applicable.	Yes	Company	Fully Covered	
65	Protection of information [mp.info]	mp.info.2 - Rating of information		Control Objective	Information classification per legal provisions (classified information per laws/treaties; OFFICIAL USE for non-classified information with handling restrictions); security policy establishes responsible persons per information; policy sets criteria for security level determination; responsible person assigns and documents security level; exclusive power to modify security level.	Yes	Company	Fully Covered	
66	Protection of information [mp.info]	mp.info.3 - Electronic signature		Control Objective	Use of any electronic signature type provided for in legal system, including secure verification code systems linked to Public Administration per Laws 39/2015 and 40/2015.	No	N/A	N/A	Tanium Cloud does not use any electronic signature type provided for in legal system
66	Protection of information [mp.info]	mp.info.3 - Electronic signature	R1	Reinforcement	Qualified certificates -- certificates shall be qualified when advanced electronic signature based on certificates is used.	No	N/A	N/A	Tanium Cloud does not use any electronic signature type provided for in legal system
66	Protection of information [mp.info]	mp.info.3 - Electronic signature	R2	Reinforcement	Algorithms and parameters authorized by the CCN or applicable national/European scheme.	No	N/A	N/A	Tanium Cloud does not use any electronic signature type provided for in legal system
66	Protection of information [mp.info]	mp.info.3 - Electronic signature	R3	Reinforcement	Verification and validation of signature guaranteed for required time, with all relevant information attached or referenced.	No	N/A	N/A	Tanium Cloud does not use any electronic signature type provided for in legal system
66	Protection of information [mp.info]	mp.info.3 - Electronic signature	R4	Reinforcement	Advanced electronic signature based on qualified certificates complemented by second factor (something known or something that is).	No	N/A	N/A	Tanium Cloud does not use any electronic signature type provided for in legal system
66	Protection of information [mp.info]	mp.info.3 - Electronic signature	R5 (optional)	Reinforcement	Qualified electronic signature using certified products per [op.pl.5].	No	N/A	N/A	Optional controls are not included in system scope
67	Protection of information [mp.info]	mp.info.4 - Time stamps		Control Objective	Time stamps applied to information usable as future electronic evidence; relevant verification data treated with same security as dated information; time stamps renewed regularly until information no longer required; qualified electronic time stamps per Regulation (EU) No 910/2014.	Yes	Company	Fully Covered	
67	Protection of information [mp.info]	mp.info.4 - Time stamps	R1 (optional)	Reinforcement	Certified products per [op.pl.5]; date and time assignment per CCN-STIC Cryptology Guide.	No	N/A	N/A	Optional controls are not included in system scope
68	Protection of information [mp.info]	mp.info.5 - Clean-up of documents		Control Objective	Removal of additional information contained in hidden fields, metadata, comments or previous revisions from documents, except where relevant to recipient. Particularly relevant for widely disseminated documents (web servers, information repositories).	Yes	Company	Fully Covered	

TANIUM

ENS Statement of Applicability

Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
69	Protection of information [mp.info]	mp.info.6 - Backups		Control Objective	Backups to recover accidentally or intentionally lost data; periodicity and retention periods determined in internal rules; procedures shall indicate: frequency, on-site storage requirements, off-site storage requirements, authorized access controls.	Yes	Company	Fully Covered	
69	Protection of information [mp.info]	mp.info.6 - Backups	R1	Reinforcement	Recovery tests -- backup and restoration procedures tested regularly; frequency depends on data criticality and lack-of-availability impact.	Yes	Company	Fully Covered	
69	Protection of information [mp.info]	mp.info.6 - Backups	R2	Reinforcement	Protection of backups -- at least one backup stored separately so incident cannot affect both original and copy simultaneously.	Yes	Company	Fully Covered	
70	Protection of services [mp.s]	mp.s.1 - E-mail protection		Control Objective	Email protection: information distributed by e-mail protected (body and annexes); message routing/connection info protected; protection against spam, harmful code (viruses, worms, Trojans, spies), micro-application mobile code (applets); rules for staff use (private communications limitations, awareness/training activities).	Yes	Company	Fully Covered	
71	Protection of services [mp.s]	mp.s.2 - Protection of web services and applications		Control Objective	Web service systems protected against: unauthorized access without authentication (preventing alternative access, URL manipulation, cookie manipulation, code injection); privilege escalation prevention; cross-site scripting prevention.	Yes	Company	Fully Covered	
71	Protection of services [mp.s]	mp.s.2 - Protection of web services and applications	R1	Reinforcement	Security audits -- continuous black-box security audits during development and before production; defined frequency.	Yes	Company	Fully Covered	
71	Protection of services [mp.s]	mp.s.2 - Protection of web services and applications	R2	Reinforcement	Advanced Security Audits -- white-box security audits during development using defined methodologies and automatic vulnerability detection tools; results analyzed and vulnerabilities resolved per [op.exp.5].	Yes	Company	Fully Covered	
71	Protection of services [mp.s]	mp.s.2 - Protection of web services and applications	R3	Reinforcement	Caches protection -- prevention of manipulation attacks on proxies and caches.	Yes	Company	Fully Covered	
72	Protection of services [mp.s]	mp.s.3 - Protection of web browsing		Control Objective	Internal user internet browsing protection: rules of use for authorized/personal use; regular browsing hygiene awareness activities; administrator training in monitoring and incident response; DNS resolution and connection info protection;	Yes	Company	Fully Covered	
72	Protection of services [mp.s]	mp.s.3 - Protection of web browsing	R1	Reinforcement	Monitoring -- web browsing use recorded with defined retention; function for encrypted channel rupture for content inspection; blacklist of closed destinations.	Yes	Company	Fully Covered	
72	Protection of services [mp.s]	mp.s.3 - Protection of web browsing	R2 (optional)	Reinforcement	Authorized destinations -- whitelist of accessible destinations with all other access prohibited.	No	N/A	N/A	Optional controls are not included in system scope
73	Protection of services [mp.s]	mp.s.4 - Protection against denial of service		Control Objective	Preventive measures against DoS and DDoS attacks: system planned and equipped with sufficient capacity with slackness; technologies deployed to prevent known attacks.	Yes	Company	Fully Covered	

ENS Statement of Applicability
Date: May 29, 2026

ENS HIGH Statement of Applicability

SCOPE: The Information Security Management System for the protection of Customer Information, Employee PII and Intellectual Property covering the infrastructure, operations, development and service activities, supporting Tanium's core platform, product modules, solutions, and cloud services.

Req	Framework Group	Control ID	Refinement	Requirement Type	Requirement Text	Applicable	Responsibility	Implementation Status	Not Applicable Rationale
73	Protection of services [mp.s]	mp.s.4 - Protection against denial of service	R1	Reinforcement	Detection and reaction -- DoS/DDoS detection and treatment system established; reaction procedures including communication with communications provider.	Yes	Company	Fully Covered	
73	Protection of	mp.s.4 - Protection against	R2	Reinforcement	Own Attacks -- detection/avoidance of attacks from own facilities	No	N/A	N/A	Optional controls are not included in system