NS1 Data Security and Privacy Principles

1. Definitions

Capitalized terms used herein have the meanings given below or if not defined below, the meanings given in the applicable written contract between NS1 and Client for the NS1 Services.

Client – is the entity to which NS1 is providing the NS1 Services under an NS1 Services Document.

Components – are the application, platform, or infrastructure elements of an NS1 Service that NS1 operates and manages.

Content – consists of all data, software, and information that Client or its authorized users provide, authorize access to, or input to NS1 Services.

DSP – is this NS1 Data Security and Privacy Principles document.

NS1 Cloud Services – are "as a service" NS1 offerings that NS1 makes available via a network, such as software as a service, platform as a service, or infrastructure as a service.

NS1 Services Document – is a Transaction Document and any other document that is incorporated into a written contract between NS1 and a Client and that addresses details of a specific NS1 Service.

NS1 Services – are (a) NS1 Cloud Services, (b) other NS1 service offerings, including infrastructure or application service offerings that NS1 delivers and dedicates to or customizes for a Client, and (c) any other services, including consulting, maintenance, or support, that NS1 provides to a Client.

Security Incident – is an unauthorized access and unauthorized use of Content.

Transaction Document – is a document that details the specifics of transactions, such as charges and a description of and information about an NS1 Cloud Service. Examples of Transaction Documents include statements of work, service descriptions, ordering documents and invoices for an NS1 Cloud Service. There may be more than one Transaction Document applicable to a transaction.

2. Overview

The technical and organizational measures provided in this DSP apply to NS1Services (including any Components) only where NS1 has expressly agreed to comply with the DSP in a written contract between NS1 and Client. For clarity, those measures do not apply where Client is responsible for security and privacy or as specified below or in an NS1 Services Document.

a. Client is responsible for determining whether an NS1 Service is suitable for Client's use and implementing and managing security and privacy measures for components that NS1 does not provide or manage within the NS1 Services. Examples of Client responsibilities for NS1 Services include: (1) the security of systems and applications built or deployed by the Client upon an infrastructure as a service or platform as a service offering or upon infrastructure, Components or software that NS1 manages for a Client, and (2) Client end-user access control and application level security configuration for a software as a service offering that NS1 manages for a Client or an application service offering that NS1 delivers to a Client.

b. Client acknowledges that NS1 may modify this DSP from time to time at NS1's sole discretion and such modifications will replace prior versions as of the date that NS1 publishes the modified version. Notwithstanding anything to the contrary in any written contract between NS1 and Client, the intent of any modification will be to: (1) improve or clarify existing commitments, (2) enable NS1 to appropriately prioritize its security focus to address evolving data and cybersecurity threats and issues, (3) maintain alignment to current adopted standards and applicable laws, or (4) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of NS1 Services.

c. In the event of any conflict between this DSP and an NS1 Services Document, the NS1 Services Document will prevail and if the conflicting terms are in a Transaction Document, they will be identified as overriding the terms of this DSP and will only apply to the specific transaction.

3. Data Protection

a. NS1 will treat all confidential and proprietary Content as confidential by not disclosing such Content except to NS1 employees, contractors, and suppliers (including subprocessors), and only to the extent necessary to deliver the NS1 Services.

b. Security and privacy measures for each NS1 Service are designed to protect confidential and proprietary Content (including Client Personal Data) processed by an NS1 Service, and to maintain the availability of such Content pursuant to the applicable written contract between NS1 and Client, including applicable NS1 Services Documents.

c. Additional security and privacy information specific to an NS1 Service may be available in the relevant NS1 Services Document or other standard documentation to aid in Client's initial and ongoing assessment of an NS1 Service's suitability for Client's use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. NS1 will direct Client to available standard documentation if asked to complete Client-preferred security or privacy questionnaires.

4. Security Policies

a. NS1 will maintain and follow written IT security policies and practices that are integral to NS1's business and mandatory for all NS1 employees. The NS1 Chief Information Security Officer will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

b. NS1 will review its IT security policies at least annually and amend such policies as NS1 deems reasonable to maintain protection of NS1 Services and Content.

c. NS1 will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly-owned NS1 subsidiaries. In accordance with NS1 internal processes and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by NS1. Each NS1 company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. NS1 employees will complete NS1's security and privacy education annually and certify each year that they will comply with NS1's ethical business conduct, confidentiality, and security policies, as set out in NS1's Business Conduct Guidelines. Additional training will be provided to any persons granted privileged access to Components that is specific to their role within NS1's operation and support of the NS1 Services, and as required to maintain compliance and accreditations stated in any relevant NS1 Services Document.

5. Compliance

a. For standard (non-custom) NS1 Cloud Services, the measures implemented and maintained by NS1 within each NS1 Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2, or both, unless stated otherwise in an NS1 Services Document.

b. Additionally, NS1 will maintain compliance and accreditation for the NS1 Services as defined in an NS1 Services Document.

c. Upon request, NS1 will provide evidence of the compliance and accreditation required by 5a. and 5b., such as certificates, attestations, or reports resulting from accredited independent third-party audits (accredited independent third-party audits will occur at the frequency required by the relevant standard).

d. NS1 is responsible for these data security and privacy measures even if NS1 uses a contractor or supplier (including subprocessors) in the delivery or support of an NS1 Service.

6. Security Incidents

a. NS1 will maintain and follow documented incident response policies consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines or equivalent industry standards for computer security incident handling and will comply with the data breach notification terms of the applicable written contract between NS1 and Client.

b. NS1 will investigate Security Incidents of which NS1becomes aware, and, within the scope of the NS1 Services, NS1 will define and execute an appropriate response plan. Client may notify NS1 of a

suspected vulnerability or incident by submitting a request through the incident reporting process specific to the NS1 Service (as referenced in an NS1 Services Document) or, in the absence of such process, by submitting a technical support request.

c. NS1 will notify Client without undue delay upon confirmation of a Security Incident that is known or reasonably suspected by NS1 to affect Client. NS1 will provide Client with reasonably requested information about such Security Incident and the status of any NS1 remediation and restoration activities.

7. Physical Security and Entry Control

a. NS1 will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into NS1 managed facilities (data centers) used to host the NS1 Services. Auxiliary entry points into such data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

b. Access to NS1-managed data centers and controlled areas within those data centers will be limited by job role and subject to authorized approval. Such access will be logged, and such logs will be retained for not less than one year. NS1 will revoke access to NS1-managed data centers upon separation of an authorized employee. NS1 will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.

c. Any person granted temporary permission to enter an NS1-managed data center facility or a controlled area within such a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

d. NS1 will take precautions to protect the physical infrastructure of NS1 managed data center facilities against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

8. Access, Intervention, Transfer and Separation Control

a. NS1 will maintain a documented security architecture for Components. NS1 will separately review such security architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense-in-depth standards prior to implementation.

b. NS1 may use wireless networking technology in its maintenance and support of the NS1 Services and associated Components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to NS1 Cloud Services networks. NS1 Cloud Services networks do not use wireless networking technology.

c. NS1 will maintain measures for an NS1 Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. NS1 will maintain appropriate isolation of its production and non-production environments, and, if Content is transferred to a non-production environment, for example to reproduce an error at Client's request, security and privacy protections in the non-production environment will be equivalent to those in production.

d. NS1 will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, or FTPS, for Client's secure transfer of Content to and from the NS1 Services over public networks.

e. NS1 will encrypt Content at rest if and as specified in an NS1 Services Document. If an NS1 Service includes management of cryptographic keys, NS1 will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

f. If NS1 requires access to Content to provide the NS1 Services, and if such access is managed by NS1, NS1 will restrict access to the minimum level required. Such access, including administrative access to any underlying Components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorized NS1 personnel following the principles of segregation of duties. NS1 will maintain measures to identify and remove redundant and dormant accounts with

privileged access and will promptly revoke such access upon the account owner's separation or upon the request of authorized NS1 personnel, such as the account owner's manager.

g. Consistent with industry standard practices, and to the extent natively supported by each Component, NS1 will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, password change frequency, and secure transfer and storage of such passwords and passphrases.

h. NS1 will monitor use of privileged access and maintain security information and event management measures designed to: (1) identify unauthorized access and activity, (2) facilitate a timely and appropriate response, and (3) enable internal and independent third-party audits of compliance with documented NS1 policy.

i. Logs in which privileged access and activity are recorded will be retained in compliance with NS1's worldwide records management plan. NS1 will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

j. To the extent supported by native device or operating system functionality, NS1 will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

k. NS1 will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with NIST guidelines for media sanitization.

9. Service Integrity and Availability Control

a. NS1 will: (1) perform security and privacy risk assessments of the NS1 Services at least annually, (2) perform security testing and vulnerability assessments of the NS1Services before production release and at least annually thereafter, (3) enlist a qualified independent third party, NS1 X-Force™ or, if specified in an NS1 Services Document, another qualified testing service to perform penetration testing of the NS1 Cloud Services, at least annually, (4) perform automated vulnerability scanning of underlying Components of the NS1 Services against industry security configuration best practices, (5) remediate identified vulnerabilities from security testing and scanning, based on associated risk, exploitability, and impact, and (6) take reasonable steps to avoid disruption to the NS1 Services when performing its tests, assessments, scans, and execution of remediation activities.

b. NS1 will maintain measures designed to assess, test, and apply security advisory patches to the NS1 Services and associated systems, networks, applications, and underlying Components within the scope of the NS1 Services. Upon determining that a security advisory patch is applicable and appropriate, NS1 will implement the patch pursuant to documented severity and risk assessment guidelines, based on Common Vulnerability Scoring System ratings of patches, when available. Implementation of security advisory patches will be subject to NS1 change management policy.

c. NS1 will maintain policies and procedures designed to manage risks associated with the application of changes to NS1 Services. Prior to implementation, changes to an NS1 Service, including its systems, networks, and underlying Components, will be documented in a registered change request that includes a description of and reason for the change, implementation details and schedule, a risk statement addressing impact to the NS1 Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

d. NS1 will maintain an inventory of all information technology assets used in its operation of NS1 Services. NS1 will continuously monitor and manage the health, including capacity, and availability of NS1 Services and underlying Components.

e. Each NS1 Service will be separately assessed for business continuity and disaster recovery requirements through appropriate business impact analysis and risk assessments intended to identify and prioritize critical business functions. Each NS1 Service will have, to the extent warranted by such risk assessments, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for an NS1 Service, if provided for in the relevant NS1 Services Document, will be established with consideration given to the NS1 Service's architecture and intended use. Physical media intended for off-site storage, if any, such as media containing backup files, will be encrypted prior to transport.