NBCUniversal
Operations & Technology
INFORMATION TECHNOLOGY
CYBER SECURITY

Third Party Security Standard

Version 5.0

Table of Contents

1. Introduction

NBCUniversal recognizes that information protection requires close cooperation between NBCUniversal and Third Parties. This Third Party Security Standard (this "Standard") outlines NBCUniversal security requirements designed to safeguard NBCUniversal Data from unauthorized or accidental modification, damage, destruction, loss or disclosure, and to protect NBCUniversal Systems.

2. Scope

These requirements are applicable to all Third Parties that: (i) manage or have access to NBCUniversal Data; (ii) have a connection to NBCUniversal Systems or the NBCUniversal network; (iii) develop custom software for NBCUniversal; or (iv) provide work product or other deliverables to NBCUniversal.

3. Establishing Security Requirements

This Standard defines the baseline information security requirements. NBCUniversal may require additional or modified requirements in the Agreement based on the nature of the Services and the risk of the engagement. Requirements set forth in this Standard apply to all Third Parties and shall not be deemed to limit any Third Party obligations under the Agreement.

4. General Security Requirements

4.1. Security Risk Assessments and Reviews

4.1.1. The Third Party must, upon request, provide confirming documentation in support of NBCUniversal's security risk assessments. Security risk assessments may include interviews; security questionnaires; examination of policies, processes, and procedures; security architecture and engineering reviews; onsite security assessments; networks and Systems assessments (third party onsite security assessments are permitted for the following IaaS/SaaS Cloud providers: Azure, Rackspace, Google, IBM and AWS); and penetration testing by NBCUniversal or its designee.

4.1.2. The Third Party must permit NBCUniversal or its designee to perform, at the expense of NBCUniversal, up to one (1) security risk assessment per year. Such risk assessment will be communicated at least three (3) months in advance, except as set forth in Section 4.3.3 of this Standard, and conducted at a time reasonably agreed upon between the Third Party and NBCUniversal. Upon request, NBCUniversal will provide the results to the Third Party.

4.1.3. The Third Party must cooperate to remediate identified Critical and High Findings and Vulnerabilities.

4.2. Personnel – Technical & Security Awareness Training

4.2.1. The Third Party must ensure that its Personnel are properly trained for the type of data, Systems and information assets they interact with including appropriate technical training.

4.2.2. The Third Party must maintain a security awareness program to address the evolving non-technical security threats introduced by human behavior. At a minimum, this program must include: (i) assembling an appropriate security awareness team; (ii) using role-based security awareness training; (iii) providing current and relevant training content for key threats such as phishing, use of privileged access and social engineering; and (iv) conducting annual security awareness training with all Third Party Personnel. Training content should be relevant to the nature of the Third Party's function and culture.

NBCUniversal reserves the right to review the program and make recommendations and improvements, where appropriate.

4.3. Incident Response

4.3.1. The Third Party must maintain an up-to-date information security incident response plan, including a process to notify and involve NBCUniversal.

4.3.2. In addition to any formal incident notification requirements set out in the Agreement, the Third Party must notify NBCUniversal, via email to cyber@nbcuni.com or via phone to the 24-Hour Incident Hotline at 1-855-650-SAFE (7233) or 1-212-664-3298, of any Security Incident. This notification to NBCUniversal must happen without unreasonable delay and in any event within 24 hours of incident confirmation. Ongoing updates about the incident must be provided as reasonably requested by NBCUniversal. Within five (5) days of closure of an incident (except where otherwise agreed by NBCUniversal in writing) the Third Party must provide a detailed incident log and root cause analysis that describes actions taken to prevent a similar event from occurring in the future.

4.3.3. In the event of a Security Incident, and upon 72 hours' notice, NBCUniversal may conduct additional security risk assessments in addition to those identified in Section 4.1 of this Standard.

4.4. Legal and Regulatory Compliance

The Third Party must comply with all Applicable Laws with respect to any software, Services and deliverables provided to NBCUniversal, and shall ensure all such software, Services and deliverables comply with Applicable Laws.

4.5. User Accounts and Access Controls

4.5.1. Third Party user accounts that may be used to access NBCUniversal Data or Systems must not be shared. Each such user account may only be assigned to one individual.

4.5.2. The Third Party must have a demonstrable identity and user account lifecycle management process, including documentation that addresses privileged account management and user account verification, deletion and disablement.

4.5.3. All NBCUniversal Data must be protected with appropriate access controls to guard against improper access, disclosure, modification, loss and deletion.

4.5.4. The Third Party shall disable the access credentials of any of the Third Party's Personnel with access to NBCUniversal Systems or NBCUniversal Data whose engagement or employment is terminated within 8 hours of the termination.

5. Application Security

5.1. Hosted Applications

If the Third Party is Hosting applications that manage NBCUniversal Data, then the Third Party shall ensure that such applications are subject to industry standard application security guidelines and, at a minimum, the Third Party must conduct regular reviews of application source code and IT infrastructure for security vulnerabilities.

5.2. External Security Reviews

The Third Party must, no less than annually, engage with an NBCUniversal-approved and qualified external organization (Qualified Security Assessor (QSA) or ISO certified services companies are pre-approved) and have that organization perform security audits of any Systems that access, transmit, receive, collect, generate, use, store, process or share Company Confidential Data or Company Restricted Data. The findings of such audit (as may be sanitized to remove information of the Third Party's other customers) must be provided to NBCUniversal upon request.

5.3. Application Audit

A Third Party Housing or Hosting Company Confidential Data or Company Restricted Data must have an established process to review the security of applications and application architecture on a regular basis (no less than semi-annually).

5.4. Application Security Program

5.4.1. The Third Party must have an established code scanning and remediation process whereby vulnerabilities are categorized and prioritized based on severity and remediated on a continual basis to reduce risk. Applications containing NBCUniversal Data, and applications located on or connected to NBCUniversal Systems or the NBCUniversal network must not contain Critical and High Findings and Vulnerabilities. NBCUniversal reserves the right to request vulnerability scans from the Third Party at any time for such applications.

5.4.2. The Third Party shall comply with secure coding standards throughout the software development life-cycle process that are consistent with the Open Web Application Security Project (OWASP) application security development controls, as may be updated by OWASP, including the Application Security Verification Standards. The Third Party's secure coding standards must include: application input validation controls; secure backend database configurations and connectivity; periodic testing; and hardening standards.

5.5. System Inventory

The Third Party must maintain an inventory of Systems that access, transmit, receive, collect, generate, use, store, process or share NBCUniversal Data.

5.6. Secure Software Delivery

5.6.1. The Third Party shall ensure that all software provided or made available to, and all software developed or maintained for, NBCUniversal follows both a secure System Development Lifecycle and a Software Development Lifecycle process and that such software is free of any known Critical and High Findings and Vulnerabilities.

5.6.2. Upon request, the Third Party shall provide access and support to NBCUniversal to perform a comprehensive application security review. Application security reviews shall cover all aspects of applications delivered to NBCUniversal, including custom code, components, products, and System configuration. Critical and High Findings and Vulnerabilities must be remediated in accordance with the Agreement and, notwithstanding anything to the contrary, as soon as reasonably required by NBCUniversal Cyber Security.

5.6.3. Security vulnerabilities, as identified by NBCUniversal Cyber Security, discovered after application delivery or release will be reported to the Third Party. The Third Party shall remediate, and retest all identified Critical and High Findings and Vulnerabilities. All ‘‘Medium’’, ‘‘Low’’ and ‘‘Informational’’ security issues, consistent with CVSS, discovered after delivery shall be handled in the same manner as other bugs and issues as specified in the Agreement.

6. Data Security

6.1. Data Management

6.1.1. The Third Party must have a demonstrable process to manage and protect NBCUniversal Data in accordance with its classification level identified by NBCUniversal, with reference to the NBCUniversal Data Classification Table in Figure 1. NBCUniversal has the right to determine and the right to reassign the data classification level on all data managed by the Third Party.

6.1.2. Upon the earlier of (a) NBCUniversal’s request or (b) 30 days after expiration or termination of the Agreement (including of an applicable statement of work or other ordering document thereunder), the Third Party must render NBCUniversal Data on the Third Party’s Systems, infrastructure and applications inaccessible, unreadable, or otherwise sanitized using a standard that meets or exceeds National Institute of Science and Technology (NIST) SP 800-88 as revised and must supply NBCUniversal with written confirmation of compliance, including, but not limited to, date of completion. If requested by NBCUniversal, the Third Party must provide NBCUniversal with all Company Confidential Data and Company Restricted Data made available to the Third Party, as well as all backup and archival media containing NBCUniversal Data.

6.2. Data Isolation

6.2.1. NBCUniversal Data that is production data must not be used in the Third Party's development or staging environment without approval from NBCUniversal Cyber Security in writing.

6.2.2. NBCUniversal Data must be separated from other Third Party customer data with the use of physical or logical controls.

6.2.3. The Third Party must not commingle Company Confidential Data or Company Restricted Data with other customer data.

6.2.4. The Third Party is responsible for all acts and omissions of its subcontractors and the use of subcontractors shall not relieve any Third Party of any responsibility under this Standard.

6.3. Data Encryption

6.3.1. Neither Company Confidential Data nor Company Restricted Data may be stored on unencrypted portable media such as laptop computers, external hard-drives, USB drives or other portable computing devices.

6.3.2. All System hard drives (e.g., laptop, workstation, and server) that contain Company Confidential Data or Company Restricted Data must be encrypted.

6.3.3. Company Confidential Data and Company Restricted Data transmitted over a public network such as the Internet must be encrypted at all times.

6.4. Backup Data

Backups of NBCUniversal Data must be managed in accordance with this Standard and returned and/or destroyed in accordance with Section 6.1.2 of this Standard or after regulatory requirements are satisfied. If retained for regulatory purposes, backup data remains subject to both this Standard and the Agreement until returned or destroyed in compliance with both this Standard and the Agreement.

7. Security Logging and Monitoring

7.1. System logging must be implemented in accordance with the criticality and sensitivity of the applicable applications, Systems and NBCUniversal Data therein, and applicable regulatory requirements. Logs must be stored, protected and reviewed as necessary for the computing environment. Security logs must be maintained for a period of at least one (1) year from recording of the applicable logs.

7.2. Logs must be made available to NBCUniversal as requested for investigation or remediation. For Systems that store, access or process Company Confidential Data or Company Restricted Data, logs must be shared with NBCUniversal's Security Information and Event Management (SIEM) environment in an automated process. If a SIEM is not available, the Third Party must remove all other customer data and share the logs promptly upon request.

8. Vulnerability Management

8.1. At NBCUniversal's discretion and direction, Systems with direct access to NBCUniversal's private network shall be subject to vulnerability assessments and remediation procedures.

8.2. The Third Party must have an established vulnerability scan and patch process whereby vulnerabilities are categorized and prioritized based on severity and remediated on a continual basis to reduce the risk. All Systems containing NBCUniversal Data, or connected to NBCUniversal, must not contain Critical and High Findings and Vulnerabilities.

8.3. All zero-day vulnerabilities must be remediated on all Systems containing NBCUniversal Data, connected to NBCUniversal, or connected to NBCUniversal Systems, within seven (7) days of announcement and/or available patch. NBCUniversal reserves the right to request vulnerability scans from the Third Party at any time for Systems or infrastructure either containing NBCUniversal Data or connecting to NBCUniversal, NBCUniversal Systems or the NBCUniversal network.

8.4. NBCUniversal reserves the right to disconnect a Third Party device should the device contain Critical and High Findings and Vulnerabilities.

8.5. The Third Party must maintain endpoint security through demonstrated provisioning, hardening, anti-malware software, and patching processes.

9. Requirement for Network Tenancy Partners

9.1. Network Connectivity Approval and Review

9.1.1. The Third Party must not make or facilitate any connections to NBCUniversal Systems or the NBCUniversal network except as approved in writing by NBCUniversal's Chief Information Security Officer ("CISO") or the CISO's designee prior to implementation.

9.1.2. All network connectivity implementations and respective justifications for connectivity may be reviewed by or on behalf of NBCUniversal and NBCUniversal may require re-approval, not more than annually. The Third Party may be required to provide additional information or alter its network connections to gain such re-approval. The Third Party acknowledges that if it fails to seek or obtain such re-approval, the Third Party may be denied access to NBCUniversal Systems and the NBCUniversal network.

9.2. Compliance and NBCUniversal Policy

Tenants must comply with the NBCUniversal Cyber Security Policy and Standards which are available from NBCUniversal Cyber Security

9.3. Audit and Reporting

NBCUniversal reserves the right to audit Tenants for compliance to NBCUniversal Cyber Security Policy and Standards.

10. Individual Contractor Requirements

10.1. Contractor Obligation

Without limitation to Section 11 of this Standard or NBCUniversal's rights under the Agreement, any violation of Section 10 of this Standard is a material breach of the Agreement and NBCUniversal reserves the right to terminate the Agreement and/or remove the Individual Contractor(s) supporting NBCUniversal on behalf the Third Party, immediately upon breach of any of these requirements.

10.2. NBCUniversal Cyber Security Policies and Standards

Individual Contractors must adhere to all NBCUniversal cyber security policies and standards, which are in the Cyber Policy Library and are accessible on the NBCUniversal Intranet. Third Party must inform their Individual Contractors about the cyber security policies and standards and their obligation to adhere.

10.3. Approved Storage Repositories

Individual Contractors must not store or copy NBCUniversal Data except as needed to perform their tasks. Individual Contractors must not forward NBCUniversal emails to alternative email domains. If data storage is required, all data must be stored in repositories owned by NBCUniversal or pre-approved, in writing, by the NBCUniversal CISO or the CISO's designee.

10.4. Security Incident Reporting

Without limitation to Section 4.3.2 of this Standard, Individual Contractors must immediately report a Security Incident via email to cyber@nbcuni.com or via phone to the 24- Hour Incident Hotline at 1-855-650-SAFE (7233).

10.5. Misuse of Devices

Individual Contractors must not misuse NBCUniversal computing devices in any manner that may undermine security, including but not limited to downloading unapproved software, disabling security monitoring tools, and visiting websites against NBCUniversal policy, as outlined in the NBCUniversal Acceptable Use Policy.

10.6. Misuse of Administrative Credentials

Individual Contractors must not misuse NBCUniversal administrative credentials in any manner that may undermine security or deviate from the designed use purpose of the credential, including but not limited to making production changes without appropriate approvals, creating or deleting accounts without formal approvals, using administrative accounts for regular business operations, sharing credentials, or taking actions with the credentials that are outside the scope of work of the Third Party, or outside the tasks assigned to that Individual Contractor.

10.7. Misuse of NBCUniversal Internet

Individual Contractors must not misuse NBCUniversal Internet. The Acceptable Use Policy is in the Cyber Policy Library, and can be accessed at any time while connected to the NBCUniversal Intranet.

10.8. Phishing Program

Individual Contractors must successfully pass the simulated phishing training program. All Individual Contractors are expected to be able to identify a simulated phishing email and must report phishing emails to NBCUniversal Cyber Security. Individuals successfully pass a simulated phishing campaign if they correctly identify the simulated phishing email, and either delete it or send to cyber@nbcuni.com without clicking on the simulated link, opening the simulated attachment, or entering their credentials on the simulated site. Immediate education is provided to all who take prohibited actions with respect to phishing emails. Without limitation to Section 11 of this Standard, repeated failure to pass a simulated phishing campaign, including the taking of prohibited actions with respect to phishing emails, shall be deemed a material breach of the Agreement.

11. Non-Compliance

Without limitation to NBCUniversal's rights under the Agreement, the Third Party's non-compliance with the requirements of this Standard (and any non-compliance for which the Third Party is responsible) shall be deemed a material breach of the Agreement. Any denial of access to NBCUniversal Systems or the NBCUniversal network arising from the Third Party's failure to comply with the terms of this Third Party Security Standard shall not excuse Third Party's performance under the Agreement

12. Definition of Key Terms

Defined terms used in this Standard shall have the meanings set forth below for purposes of this Standard:

12.1. Affiliate

Any entity that directly or indirectly, through one or more intermediaries, now or hereafter Controls, is Controlled by, or is under common Control with NBCUniversal.

12.2. Agreement

An agreement of any kind (a) into which this Standard is incorporated, by reference or otherwise (b) to which this Standard is appended or (c) in or with respect to which this Standard is otherwise included therein or made a part thereof.

12.3. Applicable Laws

All applicable laws, rules, regulations, rulings, judgments, declarations, decrees, directives, statutes, or other enactments, orders, mandates or resolutions of any governmental authority in any country or jurisdiction, and any applicable industry self-regulatory principles, in each case as may be amended or otherwise revised from time to time.

12.4. Application Security Verification Standards

The Open Web Application Security Project's Application Security Verification Standard (available at https://www.owasp.org)

12.5. Company Confidential Data

NBCUniversal Data that is "Company Confidential 3" data as defined in NBCUniversal Data Classification available from NBCUniversal Cyber Security at cyber@nbcuni.com. See Figure 1 for examples.

12.6. Company Restricted Data

NBCUniversal Data that is "Company Restricted 4" data as defined in the NBCUniversal Data Classification available from NBCUniversal Cyber Security at cyber@nbcuni.com. See Figure 1 for examples.

Level	Description	Data Examples	System Examples	Impact of Loss
COMPANY PUBLIC 1	Non-sensitive information approved and intended for public disclosure	·Press releases ·Product literature ·General information	·Static low-profile web applications ·Desktops and servers holding data as described	None
COMPANY INTERNAL 2	Information belonging to the Company and not for public disclosure	·Employee newsletters ·Awareness materials ·Marketing/Sales presentations ·Personnel policies ·Employee lists, organization charts, phone lists NBCU Work Profile available on GAL (SSO (or tied into SSO system), Location, Titles, etc.) ·3rd Party (External) Business Contact Info (Address, email, phone, etc.)	·Status low-profile web applications ·Desktops and servers holding data as described Examples: Internal or B2B systems with business contact information, no financial or contractual data	Limited harm
COMPANY CONFIDENTIAL 3	Information or systems that are sensitive or confidential to the Company and intended for internal use only on a need-to-know basis	·Company financial data ·Sales forecasts, price lists ·Customer proposals, quotes and contracts ·Strategic programs ·CMDB, Network configuration data Personal Contact Info (Address, email, phone, etc.) Demographic (Photos, Age, Date/Location of Birth, Marital Status, etc.) Profiling (IP Address, server logs, cookies data, preferences, etc. Any Personal or Employment data including salary, benefits, etc. that is not Level 2 (i.e., business contact) or Level 4 (highly sensitive) NB:Transfers of EU Individuals' or Compensation/Benefit data outside of NBCUniversal Analytics of other similar data shared with 3rd parties Online data including user location (GPS, etc.,) photos, videos, text message, etc.	·Dynamic web servers ·Desktops and servers holding data as described ·Broadcast related systems (not direct to air) Examples: Websites or mobile apps that do not process payments (NBC.com), Identity/Member management (IDX, SURF), Financial or Contract systems that do not hold Government Identifiers or Individuals	Material business harm (e.g. legal or financial liability, adverse competitive impact harm to company reputation)
COMPANY RESTRICTED 4	Information or systems that is extremely sensitive or private. Of the highest value to the Company and/or intended for use by named individuals only	Detailed financial data about company operations and profitability Medical Records Litigation and legal document PMS, passcodes/passwords Security Incidents/investigations non-public business development projects/strategy Financial (Credit/Debit Card Numbers, Bank or other Financial account Government or National Identifiers (SSN, DL, Passport, etc.) EU Special Categories (Race/Ethnicity, Trade/Union Membership, Health/Medical Records, Criminal Records, Religious/Political/Philosophical beliefs, Sexual Orientation) Biometrics	Desktops and servers holding data as described Systems involved in Broadcast (output to air) Hosts involved in pre-release film/content Point of sale High profile internet systems Examples: Financial or Contract systems with Government identifiers or individuals or company profitability details (SAP), Clinic medical systems with treatment information, websites or mobile apps that process payments (Fandango.com)	Severe harm (legal or financial liability, competitive position harm, significant loss of revenue)

Figure 1

12.7. Control

The right to exercise, directly or indirectly, the power to direct or cause the direction of the affairs, policies or management of a person, whether through the ownership of voting securities, by contract, as a trustee, or executor, or otherwise. With respect to NBCUniversal only, direct or indirect ownership of at least 20% of voting securities, equity interest or the equivalent shall also constitute Control.

12.8. Critical and High Findings and Vulnerabilities

Shall be solely defined by NBCUniversal and will be consistent with industry standards. They may be discovered or identified by NBCUniversal, or its designee, or a Third Party.

12.9. CVSS

The Common Vulnerability Scoring System.

12.10. Hosting

Providing Internet-facing servers and applications accessible by the public or NBCUniversal customers or users; most Hosting Third Parties will also be Housing NBCUniversal Data.

12.11. Housing

Storing or processing NBCUniversal Data, such as in data processing applications and backup tape storage facilities or as part of data center services. Housing includes storing NBCUniversal Data in any manner, whether accessible to the Internet or not.

12.12. Individual Contractor

Each of (a) all Third Parties that are individuals and (b) all individuals that are Personnel of a Third Party.

12.13. NBCUniversal

NBCUniversal Media, LLC and its Affiliates, including, without limitation, any signatories to the Agreement (excluding the Third Party) and any Affiliates that order, access, receive or use the Services under this Agreement.

12.14. NBCUniversal Data

All data, including NBCUniversal Personal Data and Content, in any form, that is stored, transmitted, accessed, received, collected, generated or otherwise processed by or on behalf of, or made available to, the Third Party in the course of providing Services under this Agreement, and all data regarding NBCUniversal's use of the Services. NBCUniversal Data includes NBCUniversal's confidential information and any work product or other deliverables including works in progress.

12.15. NBCUniversal Systems

All Systems owned or controlled by NBCUniversal, its Affiliates or its or their Personnel and NBCUniversal service provider or business partner Systems, (for clarity, not including the Third Party's Systems or its Personnel).

12.16. Personal Data

Any information that relates to an individual person and that, alone or in combination with other data, can be used to identify, contact, or precisely locate an individual person, or other information that constitutes "personal data" under Applicable Laws.

12.17. Personnel

A party's employees, subcontractors, vendors, agents, officers, directors and other personnel.

12.18. Security Incident

Any unauthorized access, use, damage, destruction, alteration, loss or disclosure of, NBCUniversal Data (including by or on behalf of the Third Party or its Personnel or by, on or through any of their Systems, their software or the Services).

12.19. Services

The services set forth in a statement of work or other ordering document under the Agreement, or otherwise performed under the Agreement, including the development and provision of any software, work product or other deliverables.

12.20. Systems

Websites, mobile or tablet sites, applications and other digital properties, services, platforms, software, servers, computers, hardware, firmware, middleware, networks, systems, workstations, data communications lines, routers, hubs, switches, magnetic, optical or electrical data storage devices, and all other information technology equipment.

12.21. Tenant

A Third Party that is or will be connected to NBCUniversal's private network (for instance, for purposes of illustration and not limitation, in a manner similar to a NBCUniversal remote office or through a persistent connection such as MPLS (Multi-Protocol Label Switching) or a site to site VPN).

12.22. Third Party

An entity or individual that is an NBCUniversal vendor, supplier, business partner, contractor or service provider (including, without limitation to NBCUniversal's rights under the Agreement, any subcontractors, delegates or assignees of any such parties).

13. Document Control

Document Name	Third Party Security Standard
Version	5.0
Last Reviewed	January 31, 2020

Revision History

Version	Date Released	Notes	Author	Approver
1.0	July 14, 2015	Initial version	NBCUniversal Cyber Security	NBCUniversal CISO
2.0	September 4, 2016	Added requirements for 3rd party sub-contractors and security awareness training. Removed requirement for endpoint firewalls.	NBCUniversal Cyber Security	NBCUniversal CISO
3.0	March 28, 2017	Updated to align with changes to the 3rd party MSA and other agreements; added new definitions; updated breach notification timeline; and clarified Audit/Assessment requirements	NBCUniversal Cyber Security	NBCUniversal CISO
4.0	September 27, 2018	Updated/removed document ownership, updated requirements for network connectivity and changed ‘safe’ to ‘cyber’.	NBCUniversal Cyber Security	NBCUniversal CISO
5.0	January 31, 2020	Updated requirements for user access, vulnerability management, network connectivity, individual contractors	NBCUniversal Cyber Security	NBCUniversal CISO

NBCUniversal
Operations & Technology
Cyber Security

Standard Title: Third Party Security Standard	Effective Date: 10/24/2023
	Version No.: 6.1

1. Introduction

NBCUniversal recognizes information protection requires close cooperation between NBCUniversal and Service Provider. This Third Party Security Standard (this "Standard") outlines NBCUniversal security requirements designed to safeguard NBCUniversal Data from unauthorized or accidental modification, damage, destruction, loss, or disclosure, and to protect NBCUniversal Systems.

2. Scope

These requirements are applicable to all Third Parties, including but not limited to Service Providers, that: (i) manage or have access to NBCUniversal Data; (ii) have a connection to NBCUniversal Systems or the NBCUniversal network; or (iii) provide work product or other deliverables to NBCUniversal.

3. Establishing Security Requirements

This Standard defines the baseline information security requirements. NBCUniversal may require additional or modified requirements in the Agreement based on the nature of the Services and the risk of the engagement. Requirements set forth in this Standard apply to all Third Parties and shall not be deemed to limit any Third Party obligations under the Agreement.

4. Basic Security Requirements

4.1 **Vulnerability Management.** As outlined in NIST 800-40 Rev 3 and/or ISO 27001/2, Service Provider will keep its systems and software up to date with the latest upgrades, updates, bug fixes/patches, new versions, and other modifications necessary to ensure security of the NBCUniversal Data.

4.2 **Endpoint Detection and Threat Response.** Service Provider will at all times use endpoint detection and threat response software to protect its Systems and will keep the endpoint detection and threat response software up to date. Service Provider will mitigate threats from all Viruses, spyware, and other malicious code that are or should reasonably have been detected.

4.3 **Disconnection of Third-Party Devices.** NBCUniversal reserves the right to disconnect a Service Provider device from NBCUniversal Systems should the device contain zero-day, critical, or high findings and vulnerabilities.

4.4 **Access Controls**

4.4.1 **Unique Accounts.** Service Provider user accounts that may be used to access NBCUniversal Data or Systems must not be shared. Each such user account may only be assigned to one individual.

4.4.2 **User Management.** Service Provider must have a demonstrable and documented identity and user account lifecycle management process, which addresses privileged account management and user access review, user account verification, deletion, and disablement.

4.4.3 **Account Termination**. Service Provider shall disable or enable NBCUniversal to disable the access credentials of any of the Service Provider's Personnel with access to NBCUniversal Systems or NBCUniversal Data whose engagement or employment is terminated within 24 hours of the termination.

4.4.4 **Least Privilege Access**. All NBCUniversal Data must be protected with appropriate access controls to guard against improper access, disclosure, modification, loss, and deletion.

4.4.5 **MFA.** Service Provider shall implement Modern Authentication and Multi Factor Authentication (MFA) for Personnel accessing any Internet Facing application, software, or system that accesses, transmits, receives, collects, generates, uses, stores, processes, or shares NBCUniversal Level 3 Confidential and Level 4 Restricted Data. APIs and similar Internet Facing interfaces accessing or processing NBCUniversal Data should utilize Modern Authentication with more than one authentication technique wherever technically feasible or required.

4.4.6 **Key Rotation.** If requested by NBCUniversal, Service Provider will promptly undertake encryption key and any other access credential rotation, even if this is outside of Service Provider's regular rotation schedule.

4.5 **Log Management**

4.5.1 **Retention.** Logs must be stored, protected, and reviewed as necessary for the computing environment. Except where applicable privacy laws require the redaction or deletion of Personal Data, unmodified security logs must be maintained for a period of at least one (1) year from recording of the applicable logs. Logs must be made available to NBCUniversal if requested for investigation or remediation.

4.5.2 **Log sharing.** For Systems that store, access or process Confidential Level 3 Data or Restricted Level 4 Data, logs must be shared with NBCUniversal's Security Information and Event Management (SIEM) environment in an automated process. If a SIEM is not available, Service Provider must remove all other customer data and share the logs with NBCUniversal promptly upon request.

4.6 **Subcontractors**

4.6.1 Service Provider is responsible for all acts and omissions of its Personnel and the use of Subcontractors shall not relieve any Third Party of any responsibility under this Standard.

4.6.2 Service Provider must ensure a written agreement that includes security requirements at least as protective as those set forth herein is executed between Service Provider and any Subcontractor that processes NBCUniversal Data or accesses NBCUniversal Systems as part of the Services.

4.6.3 Service Provider must conduct periodic reviews of its Subcontractors' security controls to confirm that those controls meet these security requirements.

4.6.4 In the event Service Provider identifies deficiencies in any such Subcontractor's security controls, Service Provider must maintain a report of such findings and ensure that such deficiencies are remediated within a reasonable timeframe, commensurate with their severity.

4.7 **Personnel – Technical & Security Awareness Training**

4.7.1 Service Provider must ensure that its Personnel are properly trained for the type of data, Systems and information assets they interact with, including appropriate technical training.

4.7.2 Service Provider must maintain a security awareness program in accordance with industry best practices to address the evolving security threats introduced by human behavior. Training must be at least annual, and content should be relevant to the nature of Service Provider's function and culture.

5. Data Management and Isolation

5.1 **Inventory of System.** Service Provider must maintain an inventory of Systems that access, transmit, receive, collect, generate, use, store, process or share NBCUniversal Data.

5.2 **Data Classification.** Service Provider must have a demonstrable process to manage and protect NBCUniversal Data in accordance with its classification level identified by NBCUniversal, with reference to the NBCUniversal Classification Table in Figure 1. NBCUniversal has the right to determine and reassign the data classification level on all data managed by Service Provider.

5.3 **Encryption.** Service Provider shall encrypt Confidential Level 3 Data and Restricted Level 4 Data at rest and in transit in accordance with industry best practices.

5.4 **Production Data.** Live production data (including NBCUniversal Data) must not be used in the Service Provider's development or staging environment without the prior written approval from NBCUniversal Cyber Security.

5.5 **Data Isolation.** NBCUniversal Data must be separated from other Third-Party customer data with the use of physical or logical controls.

6. Data Retention and Destruction

6.1 **Retention, Return and/or Deletion.** Unless (i) otherwise requested by NBCUniversal in writing, or (ii) Service Provider is required to retain NBCUniversal Data under Applicable Law, Service Provider must return to NBCUniversal or its designee, or at NBCUniversal's written request, securely delete, destroy or render unreadable or undecipherable all NBCUniversal Data in the possession, custody or control of Service Provider, at the earliest of the conclusion of the applicable Services, Service Provider no longer needing to process NBCUniversal Data to provide the Services, or on written instruction from NBCUniversal, and shall direct its Subcontractors to do the same. Service Provider shall promptly on NBCUniversal's request certify that such NBCUniversal Data have been returned, deleted, or destroyed. In the event of deletion, Service Provider must render NBCUniversal Data on the Service Provider's Systems, infrastructure, and applications inaccessible, unreadable, or

otherwise sanitized using a standard that meets or exceeds National Institute of Science and Technology (NIST) SP 800-88 as revised and must supply NBCUniversal with written confirmation of compliance and include the date of completion.

6.2 **Recovery.** Backups of NBCUniversal Data must be managed in accordance with this Standard and returned and/or destroyed in accordance with Section 6.1 of this Standard or after regulatory requirements are satisfied. If retained for regulatory purposes, backup data remains subject to both this Standard and the Agreement until returned or destroyed in compliance with both this Standard and the Agreement.

7. Security Review

7.1 **Certification and Risk Assessment.** Service Provider must provide NBCUniversal or its designee with third party audit certifications (preferably SOC 2- Type II, ISO 27001/2) for the relevant products or Services and/or allow NBCUniversal or its designees to perform up to one (1) security risk assessment per year as described in Section 7.2. In the event of a Security Incident or any other actual or suspected compromise of NBCUniversal Data, NBCUniversal may conduct an additional security risk assessment to verify the integrity of NBCUniversal Data and/or examine the compromised systems or processing activities. Service Provider shall fully cooperate with NBCUniversal with respect to such assessments and shall provide supporting documentation promptly on request.

7.2 **Security Risk Assessment.** NBCUniversal's security risk assessment process is an assessment of Service Provider's security standards, protocols, and relevant Systems, based on Service Provider's responses to NBCUniversal's security review questionnaire and interviews with relevant Service Provider Personnel. Service Provider has provided (and will in future provide) accurate and complete responses to such questionnaire and any other information requested as part of NBCUniversal's security risk assessment of Service Provider.

7.3 **Remediation.** If NBCUniversal identifies any material risks through the security risk assessment process, Service Provider will take all reasonable mutually agreed actions necessary to remediate or mitigate those risks within a mutually agreed upon timeframe.

8. Cyber Security Incidents

8.1 **Incident Response Plan.** Service Provider must maintain an up-to-date cyber incident response plan, which shall include a process to notify NBCUniversal of the occurrence of a Security Incident and involve NBCUniversal in addressing such incidents.

8.2 **Reporting Incidents.** In addition to any formal cyber incident notification requirements set out in the Agreement, Service Provider must notify NBCUniversal, via email to cyber@nbcuni.com with a copy to the main contact under the relevant order or via phone to the 24-Hour Incident Hotline at 1-855-650-SAFE (7233) or 1-212-664-3298, of any Cyber Security Incident. This notification to NBCUniversal must happen without unreasonable delay and in any event within 48 hours of incident confirmation.

8.3 **Incident Response.** Service Provider will a) immediately investigate and take all reasonable steps to mitigate any potential damages and remediate the cause of the Security Incident; (b) provide NBCUniversal with full details of the cause and impact of any Security Incident

(including the categories and approximate number of individuals affected and their country of residence and the categories and approximate number of records affected) and provide updates on any material developments or findings; (c) take all reasonable actions to prevent any similar reoccurrence; (d) cooperate with NBCUniversal in its efforts to investigate, remediate and mitigate the effects of the Security Incident and fulfill NBCUniversal's notification obligations; and (e) cooperate with NBCUniversal with respect to any litigation and/or investigation by or against third parties in connection with the Security Incident. Ongoing updates about the incident must be provided as reasonably requested by NBCUniversal. Within five (5) days of closure of an incident (except where otherwise agreed by NBCUniversal in writing) Service Provider must provide a detailed incident log and root cause analysis that describes actions taken to prevent a similar event from occurring in the future.

9. Application and Software Requirements

9.1 **Hosted Applications.** If Service Provider cannot provide sufficient evidence of a third-party audit certification, in accordance with Section 7.1 (Certification and Risk Assessment) of this standard, Service Provider shall ensure that such applications are subject to industry standard application security guidelines. At a minimum, Service Provider must conduct regular reviews of application source code and IT infrastructure for security vulnerabilities.

9.2 **Application Security.** Throughout the software development life-cycle process, Service Provider shall establish and comply with secure coding standards that are consistent with the Open Web Application Security Project (OWASP) application security development controls or other relevant industry standards. Service Provider's secure coding standards must be inclusive of, but not limited to application input validation controls; secure backend database configurations and connectivity; periodic testing; and hardening standards.

9.3 **Software Security.** Service Provider shall ensure that all software provided or made available to, and all software developed or maintained for, NBCUniversal follows both a secure System Development Lifecycle and a Software Development Life Cycle process.

9.4 **Delivery.** Applications and software containing NBCUniversal Data and located on or connected to NBCUniversal systems or the NBCUniversal network must not contain Critical or High Findings and Vulnerabilities at the time of delivery.

10. Requirements for Network Connectivity

10.1 **Network Connectivity Approval and Review**

10.1.1 Network Connectivity must comply with the NBCUniversal Cyber Security Policy and Standards, which are available from NBCUniversal Cyber Security (cyber@nbcuni.com). Service Provider must use NBCUniversal specified or approved methods to make or facilitate any connections to NBCUniversal Systems or the NBCUniversal network. Any deviation from such methods must be pre-approved in writing by NBCUniversal's Chief Information Security Officer ("CISO") or the CISO's designee prior to implementation of such methods.

10.1.2 All network connectivity implementations and respective justifications for connectivity may be reviewed by or on behalf of NBCUniversal and NBCUniversal may require re-approval, not more than annually. Service Provider may be required to provide additional information or alter its network connections to obtain such re-approval. Service Provider acknowledges that if it fails to seek or obtain such re-approval, Service Provider may be denied access to NBCUniversal Systems and the NBCUniversal network.

11. Contracted Personnel Requirements

This section only applies to individuals (either Service Provider's Personnel or Service Providers who are individuals) who have been issued with a SSO or granted access to NBCUniversal Systems or the NBCUniversal network (including through "desktop as a service") in order to provide the Services ("**Contracted Personnel**"). This section does not apply to Service Providers (including their Personnel) that have not been granted access to NBCUniversal Systems or the NBCUniversal network.

11.1 **NBCUniversal Cyber Security Policies and Standards**
Contracted Personnel must adhere to all NBCUniversal cyber security policies and standards, (including the Acceptable use Policy) which are in the Cyber Policy Library and are accessible on the NBCUniversal Intranet. Service Provider must instruct their Contracted Personnel to adhere to the cyber security policies.

11.2 **Approved Storage Repositories**
Contracted Personnel must not store or copy NBCUniversal Data except as needed to perform the Services. Contracted Personnel must not forward NBCUniversal emails to alternative email domains or take any other actions designed to move or copy NBCUniversal Data to any location not pre-approved, in writing, by the NBCUniversal CISO or the CISO's designee. If data storage is required, all data must be stored in repositories owned by NBCUniversal or pre-approved, in writing, by the NBCUniversal CISO or the CISO's designee.

11.3 **Security Incident Reporting**
Without limitation to Section 8.2 of this Standard, Contracted Personnel must immediately report a Security Incident via email to cyber@nbcuni.com or via phone to the 24-Hour Incident Hotline at +1-855-650-SAFE (7233).

11.4 **Misuse of Devices**
Contracted Personnel must not use NBCUniversal computing devices in any manner that may undermine security, including but not limited to such acts as downloading unapproved software, disabling security monitoring tools.

11.5 **Misuse of Administrative Credentials**
Contracted Personnel must not use NBCUniversal administrative credentials in any manner that may undermine security or deviate from the designed use purpose of the credential, including but not limited to making production changes without appropriate approvals, creating or deleting accounts without formal approvals, using administrative accounts for regular business operations, sharing credentials, or taking actions with the credentials that

are outside the scope of work of Service Provider, or outside the tasks assigned to that Contracted Personnel.

11.6 **Misuse of NBCUniversal Intranet**
Contracted Personnel must not misuse the NBCUniversal Intranet.

11.7 **Phishing Program**
Contracted Personnel must successfully pass the simulated phishing training program and report suspicious emails to cyber@nbcuni.com. Failure of phishing exercises will result in immediate education.

12. Non-Compliance

Without limitation to NBCUniversal's rights under the Agreement, Service Provider's non-compliance with the requirements of this Standard (and any non-compliance for which Service Provider is responsible) shall be deemed a material breach of the Agreement. Any denial of access to NBCUniversal Systems or the NBCUniversal network arising from Service Provider's failure to comply with the terms of this Third Party Security Standard shall not excuse Service Provider's performance under the Agreement.

13. Definition of Key Terms

Defined terms used in this Standard shall have the meanings set forth below for purposes of this Standard:

13.1 **Affiliate**
Any entity that directly or indirectly, through one or more intermediaries, now or hereafter Controls, is Controlled by, or is under common Control with NBCUniversal.

13.2 **Agreement**
An agreement of any kind (a) into which this Standard is incorporated, by reference or otherwise (b) to which this Standard is appended or (c) in or with respect to which this Standard is otherwise included therein or made a part thereof.

13.3 **Applicable Laws**
All applicable laws, rules, regulations, rulings, judgments, declarations, decrees, directives, statutes, or other enactments, orders, mandates, or resolutions of any governmental authority in any country or jurisdiction, and any applicable industry self-regulatory principles, in each case as may be amended or otherwise revised from time to time.

13.4 **Confidential Level 3 Data**
NBCUniversal Data that is "Confidential Level 3" data as defined in the Data Classification Table available from NBCUniversal Cyber Security at cyber@nbcuni.com. See Figure 1 for examples.

13.5 **Control**
The right to exercise, directly or indirectly, the power to direct or cause the direction of the affairs, policies, or management of a person, whether through the ownership of voting securities, by contract, as a trustee, or executor, or otherwise. With respect to NBCUniversal

only, direct, or indirect ownership of at least 20% of voting securities, equity interest or the equivalent shall also constitute Control.

13.6 **Critical and High Findings and Vulnerabilities**
Shall be solely defined by NBCUniversal and will be consistent with industry standards (CVSS). They may be discovered or identified by NBCUniversal, or its designee, or a Third Party.

13.7 **CVSS**
The Common Vulnerability Scoring System.

13.8 **Contracted Personnel**
Individuals (either Service Provider's Personnel or Service Providers who are individuals) who have been issued with a SSO or granted access to NBCUniversal Systems or the NBCUniversal network (including through "desktop as a service") in order to provide the Services.

13.9 **Figure 1 Data Classification Table**

		Sensitive Information		
Data Class Name	**Public**	**Internal**	**Confidential**	**Restricted**
Tier Designation	**1**	**2**	**3**	**4**
Description	Information approved for public release.	Information meant for internal use only. Limited to internal NBCUniversal access and distribution.	Information available on a need-to-know basis only. Limited internal access and distribution.	Regulated information or otherwise reserved for use by named individuals only. Most limited internal access and distribution.
Typical Data Types (this is not meant to be a complete list)	Information specifically intended for public release	• Sales strategies • Organizational charts • Business contact data	• Intellectual property • Employee information • Contracts • Risk, threat, vulnerability information	• Pre-release content • Intellectual property • Security credentials (biometrics, passwords, access keys, etc.) • PCI (financial) • Consumer Information • Personal Data • Sensitive Personal Information

13.10 **Internet Facing**

Programs and Services that are accessible from the internet.

13.11 **Modern Authentication**
Multi-functional authorization methods that use modern authentication protocols (e.g., SAML, OICD, OAuth, etc.) and are able to apply continuous risk-based access policies and utilize modern authentication methods (e.g., passwordless, FIDO, biometrics, etc.)

13.12 **Multifactor Authentication (MFA)**
An electronic authentication method that requires a user to present two or more pieces of

evidence (factors) to an authentication mechanism to gain access to a website, application, or resource. Factors include: (i) something you know [e.g., password/personal identification number (PIN)]; (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor authentication must be performed using a multifactor authenticator or by a combination of authenticators that provides different factors.

13.13 **NBCUniversal**
NBCUniversal Media, LLC and its Affiliates, including, without limitation, any signatories to the Agreement (excluding Service Provider) and any Affiliates that order, access, receive or use the Services under the Agreement.

13.14 **NBCUniversal Systems**
All Systems owned or controlled by NBCUniversal, its Affiliates or its or its Personnel and NBCUniversal service provider or business partner Systems, (for clarity, not including the Third Party's Systems or its Personnel).

13.15 **NBCUniversal Data**

Any data or content of NBCUniversal, its Affiliates, and its respective Personnel and licensors, including NBCUniversal Personal Data, feature and television assets, clips, dailies, scripts, music, marketing materials, final cuts, rough cuts, trailers, audio elements, pictures, graphics, logos, software, specifications, designs, works in progress or other creative works, that is stored, transmitted, accessed, received, collected, generated or otherwise processed by or on behalf of, or made available to, Service Provider in the course of providing Services.

13.16 **NBCUniversal Personal Data**
Personal Data that is processed by, or made available to, Service Provider in the course of providing Services under the Agreement.

13.17 **Network Connectivity**
Any connection to NBCUniversal's private network (for instance, for purposes of illustration and not limitation, in a manner similar to a NBCUniversal remote office or through a persistent connection such as MPLS (Multi-Protocol Label Switching) or a site-to-site VPN).

13.18 **Personal Data**

Any information that relates to an individual person and that, alone or in combination with other data, can be used to identify, contact, or precisely locate an individual person, or other information that constitutes "personal data" or "personal information" under Applicable Laws.

13.19 **Personnel**
A party's employees, subcontractors, vendors, agents, officers, directors, and other personnel. References to a party include its Personnel.

13.20 **Restricted Level 4 Data**
NBCUniversal Data that is "Restricted Tier 4" data as defined in the Data Classification Table available from NBCUniversal Cyber Security at cyber@nbcuni.com. See Figure 1 for examples.

13.21 **Security Incident or Cyber Security Incident**
Any accidental, unlawful, or unauthorized access, use, damage, destruction, alteration, loss, or disclosure of, NBCUniversal Data (including by or on behalf of Service Provider or its Personnel or by, on or through any of its Systems, its software or the Services or Deliverables).

13.22 **Services**
The services set forth in a statement of work or other ordering document under the Agreement, or otherwise performed under the Agreement, including the development and provision of any software, work product or other deliverables.

13.23 **Subcontractor**
Any external party, including Service Provider's Affiliates and subcontractors, appointed by Service Provider to process NBCUniversal Data.

13.24 **Systems**
Websites, mobile or tablet sites, applications and other digital properties, services, platforms, software, servers, computers, hardware, firmware, middleware, networks, systems, workstations, data communications lines, routers, hubs, switches, magnetic, optical, or electrical data storage devices, and all other information technology equipment.

13.25 **Service Provider**
An entity that has contracted with NBCUniversal to provide Services under the Agreement.

13.26 **Third Party**

An entity or individual that is an NBCUniversal vendor, supplier, business partner, contractor, or Service Provider (including without limitation to NBCUniversal's rights under the Agreement, any Personnel, delegates, or assignees of any such parties).

13.27 **Viruses**

Virus means any virus, worm, "back door," "Trojan Horse," drop dead device, time bomb, spyware, adware or other malicious, harmful, destructive, or disruptive code, component or device, including any code, component or device that may cause a Security Incident or damages to Systems, or is capable of facilitating any of the foregoing.