NBCUniversal
Operations & Technology
Cyber Security

Standard Title: Third Party Security Standard	Effective Date: 3/15/2023
	Version No.: 6.0

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 Company Content 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 Company Content; (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. Basic Security Requirements

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

4.2 **Endpoint Detection and Threat Response.** Third Party will at all times use endpoint detection and threat response software and will keep the endpoint detection and threat response software up to date. Third Party 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 Third-Party device should the device contain Zero-Day, Critical, and High Findings and Vulnerabilities.

4.4 **Encryption.** Third Party shall encrypt Confidential Data and Restricted Data at rest and in transit in accordance with industry best practices.

4.4.1 NBCUniversal reserves the right to request encryption key and any other access credential rotation outside of Third Party's regular rotation schedule.

4.5 **Access Controls**

4.5.1 Third Party user accounts that may be used to access Company Content 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 access review, user account verification, deletion and disablement.

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

4.5.4 The Third Party shall implement Modern Authentication and Multi Factor Authentication (MFA) for any public facing application, software, or system that accesses, transmits, receives, collects, generates, uses, stores, processes, or shares Company Content.

4.5.5 Logs must be stored, protected and reviewed as necessary for the computing environment. Unless prohibited by applicable privacy laws, 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 as requested for investigation or remediation.

4.5.6 For Systems that store, access or process Confidential Data or 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.

4.6 **Subcontractors.** 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.

4.7 **Account Termination.** The Third Party shall disable or enable NBCUniversal to disable the access credentials of any of the Third Party's Personnel with access to NBCUniversal Systems or Company Content whose engagement or employment is terminated within 24 hours of the termination.

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

4.8.1 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.

4.8.2 The Third Party must maintain a security awareness program in accordance with industry best practices to address the evolving security threats introduced by human behavior. Training content should be relevant to the nature of the Third Party's function and culture.

4.9 **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.

5. Data Management and Isolation

5.1 **Inventory of System.** The Third Party must maintain an inventory of Systems that access, transmit, receive, collect, generate, use, store, process or share Company Content.

5.2 **Data Classification.** The Third Party must have a demonstrable process to manage and protect Company Content in accordance with its classification level identified by NBCUniversal, with reference to the Company Content 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.

5.3 **Production Data.** Company Content 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. Under no circumstances shall Service Provider use live production NBCUniversal Personal Data for testing purposes.

5.4 **Data Isolation.** Company Content 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) Third Party is required to retain it under Applicable Law, Third Party must return to NBCUniversal or its designee, or at NBCUniversal's written request, securely delete, destroy or

render unreadable or undecipherable all Company Content in the possession, custody or control of Third Party, at the conclusion of the applicable Services or on written instruction from NBCUniversal, and shall direct its subcontractor to do the same. Third Party shall promptly on NBCUniversal's request certify that such NBCUniversal l Data has been returned, deleted or destroyed. In the event of deletion, the Third Party must render Company Content 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.

6.2 **Recovery.** Backups of Company Content 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.** The Third Party must provide NBCUniversal or its designee with third party audit certifications (preferably SOC 2- Type II, ISO 27001/2) for the related products or services and/or allow NBCUniversal or its designees to perform, at the expense of NBCUniversal, up to one (1) security risk assessment per year. Third Party shall, upon request, provide confirming documentation in support of NBCUniversal's security risk assessments.

7.2 **Review.** NBCUniversal may at its discretion conduct (and may have conducted prior to the Effective Date) reviews of Third Party's security standards, protocols and relevant Systems, including interviews with relevant Third Party Personnel, and as part of such a review NBCUniversal may require Third Party to provide responses to NBCUniversal's security review questionnaire (each such review, an "NBCUniversal Supplier Security Review," and each such questionnaire, a "Supplier Security Review Questionnaire"). Third Party has provided (and will in future provide) accurate and complete responses to the Supplier Security Review Questionnaire and any other information requested as part of NBCUniversal's diligence review of Third Party.

7.3 **Remediation.** If any security risk assessment identifies any deficiencies, Third Party will take all reasonable actions necessary to remediate those deficiencies within a mutually agreed upon timeframe.

8. Cyber Security Incidents

8.1 **Incident Response Plan.** The Third Party must maintain an up-to-date cyber incident response plan, including a process to notify and involve NBCUniversal.

8.2 **Reporting Incidents.** In addition to any formal cyber incident notification requirements set out in the Agreement, the Third Party 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. The Third Party 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 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 its 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) 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.

9. Application and Software Requirements

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

9.2 **Application Security.** The Third Party shall establish and 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 or other relevant industry standards.

9.3 **Software Security.** 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.

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

10. Requirements for Network Connectivity

10.1 **Network Connectivity Approval and Review**

10.1.1 The Third Party must use NBCUniversal approved methods to make or facilitate any to connections to NBCUniversal Systems or the NBCUniversal network. Any deviation must be approved in writing by NBCUniversal's Chief Information Security Officer ("CISO") or the CISO's designee prior to implementation.

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. 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.

10.2 **Compliance and NBCUniversal Policy.** Network Connectivity must comply with the NBCUniversal Cyber Security Policy and Standards, which are available from NBCUniversal Cyber Security.

10.3 **Audit and Reporting.** NBCUniversal reserves the right to audit Network Connectivity for compliance to NBCUniversal Cyber Security Policy and Standards.

11. Individual Contractor Requirements

(Section 11 is only applicable to Individual Contractors, in all other instances this section is not appliable.)

11.1 **Contractor Obligation**
Without limitation to Section 12 of this Standard or NBCUniversal's rights under the Agreement, any violation 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.

11.2 **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.

11.3 **Approved Storage Repositories**
Individual Contractors must not store or copy Company Content except as needed to perform their tasks. Individual Contractors must not forward NBCUniversal emails to alternative email domains or take any other actions designed to move Company Content 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.

11.4 **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).

11.5 **Misuse of Devices**
Individual Contractors must not use 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.

11.6 **Misuse of Administrative Credentials**

Individual Contractors 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 the Third Party, or outside the tasks assigned to that Individual Contractor.

11.7 **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.

11.8 **Phishing Program**
Individual Contractors must successfully pass the simulated phishing training program. All Individual Contractors are expected to be able to identify a simulated or real 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 report it 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 12 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.

12. Non-Compliance

12.1 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.

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 **Company Content**

Any data, user data or content of Company, its Affiliates, and their respective Personnel and licensors, including 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. For the avoidance of doubt, Company Content does not include Company Personal Data.

13.5 **Confidential Data**

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

13.6 **Restricted Data**

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

		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 for public release	• Sales strategies • Organizational charts • Business contact data	• Intellectual property • Employee information • Consumer Information • Contracts • Risk, threat, vulnerability information	• Intellectual property • Security credentials (biometrics, passwords, access keys, etc.) • PCI (financial) • Personal Data • Sensitive Personal Information

Figure 1

13.7 **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.

13.8 **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.

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

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

13.11 **Modern Authentication**
Modern authentication is an umbrella term for a combination of authentication and authorization methods between a client (for example, your laptop or your phone) and a server, as well as some security measures that rely on access policies that you may already be familiar with.

13.12 **Multifactor Authentication (MFA)**
Authentication that requires more than one distinct authentication factor for successful authentication. 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 can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors.

13.13 **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 the Agreement.

13.14 **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).

13.15 **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.

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

13.17 **Security Incident or Cyber Security Incident**
Any accidental, unlawful, or unauthorized access, use, damage, destruction, alteration, loss or disclosure of, Company Content (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 or Deliverables).

13.18 **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.

13.19 **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.

13.20 **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).

13.21 **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).

13.22 **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.

14. Approval

Approved by: Senior Vice President and Chief Information Security Officer

Approval Date: 03/15/2023

Electronic approval on file with GRC Policy

15. Revision History

Version	Changes	Approved	Published	Effective
1.0	Initial version	7/14/2015	7/14/2015	7/14/2015
2.0	Added requirements for 3rd party subcontractors and security awareness training. Removed requirement for endpoint firewalls.	9/4/2016	9/4/2016	9/4/2016
3.0	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.	3/28/2017	3/28/2017	3/28/2017
4.0	Updated/removed document ownership, updated requirements for network connectivity and changed 'safe' to 'cyber.'	9/27/2018	9/27/2018	9/27/2018
5.0	Updated requirements for user access, vulnerability management, network connectivity, individual contractors.	1/31/2020	1/31/2020	1/32/202
6.0	Extensive refresh of entire document including: • Incorporated requirements from the MVP document. Details listed in the *Executive Summary for Third Party Security Standard v 6.0.* • Incorporated requirements from the Peacock agreement. Details listed in the *Executive Summary for Third Party Security Standard v 6.0.* • Some portions of the previously published version (v 5.0) have been removed so that the standard is less prescriptive. The removed content is listed in detail in the *Executive Summary for Third Party Security Standard v 6.0.* • For consistency with *Data Management* standard v 6.0 (expected publication Q2 2023) removed "company" from the names of the data classification levels so they are now: Level 1 Public, Level 2 Internal, Level 3 Confidential, and Level 4 Restricted. • Updated the formatting, look, and feel of the document for consistency with the newer versions of cyber security standards being published.	3/15/2023	3/15/2023	3/15/2023