Contents

1. Introduction 1
2. Scope 1
3. Establishing Security Requirements 1
4. Basic Security Requirements 2
5. Data Management and Isolation 4
6. Data Retention and Destruction 4
7. Security Review 4
8. Security Incidents 5
9. Application and Software Requirements 5
10. Artificial Intelligence 6
11. Requirements for Network Connectivity 6
12. Contracted Personnel Requirements 6
13. Content Protection 7
14. Non-Compliance 8
15. Definition of Key Terms 8
16. Approval 12
17. Revision History 12

1. Introduction

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

2. Scope

These requirements are applicable to all Service Providers that: (i) manage or have access to Company Data; (ii) have a connection to Company Systems or the Company network; (iii) provide or create work product or other deliverables to Company; or (iv) receive Company Content.

3. Establishing Security Requirements

This Standard defines the baseline information security and content security requirements. Company 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 Service Providers and shall not be deemed to limit any Service Provider obligations under the Agreement.

4. Basic Security Requirements

4.1 **Security Policies**. Service Provider will maintain written information security policies, standards and procedures that (a) meet legal and regulatory requirements, (b) meet the requirements herein, and (c) include evaluation of insider threats and implement a plan to mitigate these threats. Policies, standards, and procedures must be reviewed regularly and updated as required, including after a Security Incident and whenever a material change is made that affects your security program.

4.2 **Vulnerability Management.** As outlined in NIST 800-40 Rev 4 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 the security of Company Data.

4.3 **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.

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

4.5 **Access Controls**

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

4.5.2 **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.

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

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

4.5.5 **ID Verification.** Service Provider shall maintain processes reasonably designed to verify the identity and employment status of Personnel prior to granting access to Company Data, Systems, Networks or facilities. Such processes shall include identity verification, prior employment verification, onboarding validation procedures, or other comparable measures appropriate to the nature of the Services and Service Provider shall provide evidence of same upon request.

4.5.6 **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 Confidential Level 3 Data and Sensitive Non-Public Level

4 Data. APIs and similar Internet Facing interfaces accessing or processing Company Data should utilize Modern Authentication with more than one authentication technique wherever technically feasible or required.

4.5.7 **Key Rotation.** If requested by Company, 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.

4.6 **Log Management**

4.6.1 **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 Company upon request for investigation or Remediation.

4.6.2 **Log sharing.** For Systems that store, access, or process Confidential Level 3 Data or Sensitive Non-Public Level 4 Data, logs must be shared with Company'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 Company promptly upon request.

4.7 **Subcontractors**

4.7.1 Service Provider is responsible for all acts and omissions of its Personnel and the use of Subcontractors shall not relieve any Service Provider of any responsibility under this Standard including, but not limited to, reporting Subcontractor Security Incidents that impact or have the potential to impact Company.

4.7.2 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 Company Data or accesses Company Systems as part of the Services.

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

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

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

4.8.1 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.

4.8.2 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.

4.9 **Physical Security.** Entry/exit points of Service Provider facilities must be secure at all times, including loading dock doors (if applicable) and windows.

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 Company Data.

5.2 **Data Classification.** Service Provider must have a demonstrable process to manage and protect Company Data in accordance with its classification level identified by Company, with reference to the Company Classification Table in Figure 1. Company 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 Sensitive Non-Public Level 4 Data at rest and in transit in accordance with industry best practices.

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

5.5 **Data Isolation.** Company 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 Company in writing, or (ii) Service Provider is required to retain Company Data under Applicable Law, Service Provider must return to Company or its designee, or at Company's written request, securely delete, destroy, or render unreadable or undecipherable all Company 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 Company Data to provide the Services, or on written instruction from Company, and shall direct its Subcontractors to do the same. Service Provider shall promptly on Company's request certify that such Company Data have been returned, deleted, or destroyed. In the event of deletion, Service Provider must render Company 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 Standards and Technology (NIST) SP 800-88 as revised and must supply Company with written confirmation of compliance and include the date of completion.

6.2 **Recovery.** Backups of Company 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 Company 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 Company 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 Company Data, Company may conduct an additional security risk assessment to verify the integrity of Company Data and/or examine the compromised systems or processing activities. Service Provider shall

fully cooperate with Company with respect to such assessments and shall provide supporting documentation promptly on request.

7.2 **Security Risk Assessment.** Company'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 Company'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 Company's security risk assessment of Service Provider.

7.3 **Remediation.** If Company 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. 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 Company of the occurrence of a Security Incident and involve Company 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 Company, 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 Company must happen without unreasonable delay and in any event within 24 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 Company 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 Company in its efforts to investigate, Remediate and mitigate the effects of the Security Incident and fulfill Company's notification obligations; and (e) cooperate with Company 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 Company. Within five (5) days of closure of an incident (except where otherwise agreed by Company 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, Company follows both a secure System Development Lifecycle and a Software Development Life Cycle process.

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

10. Artificial Intelligence

10.1 Without prior written authorization from Company in a Scope of Work attached to the Agreement, Service Provider shall not, and shall ensure that it and any Subcontractor, and their respective employees shall not use confidential information, Intellectual Property, or other Company Data for the purposes of training, tuning, developing, testing, or improving any Artificial Intelligence System.

11. Requirements for Network Connectivity

11.1 **Network Connectivity Approval and Review**

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

11.1.2 All network connectivity implementations and respective justifications for connectivity may be reviewed by or on behalf of Company and Company 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 Company Systems and the Company network.

12. 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 Company Systems or the Company 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 Company Systems or the Company network.

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

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

12.3 **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).

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

12.5 **Misuse of Administrative Credentials**
Contracted Personnel must not use Company 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.

12.6 **Misuse of Company Intranet**
Contracted Personnel must not misuse the Company Intranet.

12.7 **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.

13. Content Protection

This section only applies to engagements involving Company Intellectual Property and Company Content. Content protection requirements follow best practices as established by the Motion Picture Association (MPA).

13.1. **Subcontractors.** If the Service Provider is responsible for handling Company Content, Service Provider must obtain written permission from FilmAndTVSecurity@nbcuni.com prior to engaging Subcontractors to perform any Services.

13.2. **Facility Access Authorization.** Access of visitors, contractors, and vendors to facility premises shall require a visitor log and issuance of temporary badges. Visitors, vendors, and contractors must be escorted and/or supervised at all times while present at a facility.

13.3. **Physical Security.** Sign-in logs shall be retained for a minimum of one (1) year, temporary badges must be distinct from employee badges and visitor badges; visitors, contractors and vendors must not be provided with key card access to content/production areas of a Facility.

13.4. **Electronic Access Control.** Electronic access must be implemented throughout the facility to cover all entry/exit points and all areas where Company Content are stored, transmitted, or

processed. Electronic access must be assigned to specific facility areas based on job function and responsibilities and updated accordingly when roles change upon termination of company personnel and third-party workers. System administration shall be restricted to appropriate personnel.

13.5. **Electronic Devices.** Devices issued to a third party must have an expiration date based on an approved timeframe. Lost or stolen electronic access devices shall be immediately deactivated before issuing a new device.

13.6. **Closed Circuit Television Cameras.** Service Provider shall have closed circuit television cameras at (a) all entries and exits to all buildings in the Facility, including vehicle entry, exit points and emergency exits, and (b) all storage areas, server rooms, vaults, and devices storing content. Footage shall be retained and stored digitally in a secure location for at least 90 days, or the maximum retention period allowed by law. Cameras shall be maintained in proper working order at all times.

13.7. **Equipment and Asset Management.** To the extent Service Provider has physical equipment and assets, Service Provider shall ensure (a) recording equipment used to dub or clone materials and backups shall be located in a secure area with restricted access; (b) all blank media, including hard drives, LTOs, etc., shall be kept in a secure location with restricted access and to also include inventory of assets, (c) workflow with respect to materials shall be monitored regularly and audited periodically.

13.8. **Content Security.** If the Service Provider receives or delivers Company Content, including but not limited to work product, proprietary material, or confidential information related to Company's Intellectual Property, Service Provider must complete an additional content-based assessment.

13.9. **Incident Response.** Service Provider shall complete remedial steps as described in Section 8.3 within five (5) days in the event of a Company Content or Company Intellectual Property-related incident.

13.10. **Remediation.** In the event Company Content or Company Intellectual Property-related incidents are not remediated within five (5) days of notice to Company's satisfaction, Company may terminate all Services without further obligation or liability to the Service Provider except with respect to agreed compensation for any previously rendered Services unrelated to the Security Incident.

14. Non-Compliance

Without limitation to Company'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 Company Systems or the Company 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.

15. Definition of Key Terms

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

15.1. **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 Company.

15.2. **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.

15.3. **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.

15.4. **Company**
The NBCUniversal party to the Agreement 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.

15.5. **Company Content**
Any data, user data, and/or materials and assets related to film or television properties of Company, its Affiliates, and their respective Personnel and licensors, including any inputs, prompts, final cuts, rough cuts, trailers, clips, dailies, scripts, sides, stills, breakdowns, budgets, call sheets, music, marketing and promotional materials, consumer products, audio elements, key art, pictures, graphics, logos, posters, auditions, plot points, spoilers, character designs, storyboards, drawings, software, specifications, designs, works in progress or other data or creative works (including all associated metadata), sensitive production legal and finance documents, and confidential information related to Company Intellectual Property that is inputted, stored, transmitted, accessed, received, collected, generated, or otherwise processed by or made available to Service Provider by or on behalf of Company as part of the Services.

15.6. **Company Data**
Any data of Company, its Affiliates, and their respective Personnel and licensors that is inputted, stored, transmitted, accessed, received, collected, generated or otherwise processed by, or made available to, Service Provider as part of the Services, including Company Personal Data and Company Content.

15.7. **Company Intellectual Property**
Any (a) trademarks, service marks, trade names, trade dress and Internet domain names, together with all goodwill and common law rights associated therewith; (b) patents; (c) copyrights; (d) registrations and applications for registration of any of the foregoing in (a)-(c); (e) trade secrets; and (f) rights of privacy and/or publicity; and all other forms of intellectual property or proprietary rights, and derivatives thereof.

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

15.9. **Company Systems**
All Systems owned or controlled by Company, its Affiliates or its Personnel, and Company service provider or business partner Systems, (for clarity, not including the Service Provider's Systems or its Personnel).

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

15.11. **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 Company Systems or the Company network (including through "desktop as a service") in order to provide the Services.

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

15.13. **Critical and High Findings and Vulnerabilities**
Shall be solely defined by Company and will be consistent with industry standards (CVSS). They may be discovered or identified by Company, or its designee, or a Service Provider.

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

15.15. **Figure 1 Data Classification Table**

Data Class Name			Cyber Sensitive Information		
	Non-Business	Public	General Business	Confidential	Sensitive Non-Public
Tier	0	1	2	3	4
Description	Information that is not business-related or information that is personal, such as information generated or shared pursuant to Company's *Acceptable Use Policy* for incidental personal use. Company does not generally control access to Non-Business Information.	Information approved for public release or that, if disclosed, would cause no harm to Company.	Information meant for internal use only. Limited to internal Company access and distribution. Business information that is not approved for public circulation, where the loss of confidentiality, integrity, or availability of such information could be expected to have a **limited adverse effect (as defined in the Glossary)** on Company operations, organizational assets, or individuals.	Information available on a need-to-know basis only. Limited internal access and distribution. Confidential information, not intended for public release, where the loss of confidentiality, integrity, or availability of such information could be expected to have a **serious adverse effect (as defined in the Glossary)** on Company operations, organizational assets, or individuals.	Regulated information or otherwise reserved for use by named individuals only. Most limited internal access and distribution, where the loss of confidentiality, integrity, or availability of such Information could be expected to have a **severe adverse effect (as defined in the Glossary)** on Company operations, organizational assets, or individuals.
Typical Data Types (this is not meant to be a complete list)	• Dinner plans with spouses, children, work colleagues, or friends • Children's school schedules	Information specifically for public release	• Sales strategies • Organizational charts Business Contact Personal Information[1] (e.g., vendors we work with and workforce information in GAL)	• Intellectual property • Workforce information (excluding SPI) • Contracts Risk, threat, vulnerability information	• Pre-release content • Intellectual property* • Security credentials (biometrics, passwords, access keys, etc.) • All other personal information (direct and indirect identifiers and SPI) • Specific risk, threat, vulnerability

Data Class Name			Cyber Sensitive Information		
					information

15.16. **Internet Facing**
Programs and Services that are accessible from the internet.

15.17. **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.)

15.18. **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.

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

15.20. **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.

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

15.22. **Remediation**
The neutralization or elimination of a vulnerability or its likelihood of exploitation.

15.23. **Security Incident**
Any accidental, unlawful, or unauthorized access, use, damage, destruction, alteration, loss, or disclosure of, Company Data, Company Content, and/or Company Intellectual Property (including by or on behalf of Service Provider, its Personnel, subcontractors, or by, on or through any of its Systems, its software or the Services or Deliverables).

15.24. **Sensitive Non-Public Level 4 Data**
Company Data that is "Sensitive Non-Public Level 4" data as defined in the Data Classification Table available from Company Cyber Security at cyber@nbcuni.com. See Figure 1 for examples.

15.25. **Service Provider**
An entity or individual that has contracted with Company to provide Services under the Agreement.

15.26. **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.

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

15.28. **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.

15.29. **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.

16. Approval

Approved by: George Ressopoulos, Senior Vice President, and Chief Information Security Officer

Approval Date: 10/16/2026 (*Electronic approval on file with Cyber Policy)*

17. 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	1/31/2020

Version	Changes	Approved	Published	Effective
6.0	Extensive refresh of entire document including: • Incorporated requirements from the MVP document. Details listed in *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 the *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 newer versions of cyber security standards being published.	3/15/2023	3/15/2023	3/15/2023
6.1	Updated to add definition and reference to "Company Personal Data" any time "Company Content" is referenced. Added definition for Public-Facing. Updated Data Classification table.	10/24/2023	10/24/2023	10/24/2023
6.2	Updated the Data Classification footer & added the Last Reviewed Date in the header.	09/16/2025	09/16/2025	09/16/2025
7.0	Highlights (moderate impact): Added Section 10 Artificial Intelligence. Added Section 13 Content Protection.	12/11/2025	12/19/2025	12/19/2025
7.1	Highlights: Added Section 4.5.5 ID Verification, requiring Service Providers to verify the identity and employment status of Personnel prior to granting access to Company Data, Systems, Networks or facilities. Updated the Section 15.4 definition of Company to the NBCUniversal party to the Agreement and its Affiliates.	11/6/2026	11/06/2026	11/06/2026