Schedule [A]
Data Processing Addendum

Template Name: Data Processing Addendum
Template Date: February 13, 2026
Region for Use: Global
Restrictions: None
Additional Notes: Additional information found in the NBCU Privacy Playbook. This template may be used for any agreement involving the processing of personal data. Certain processing activities may have additional requirements. This document is self-contained and can be attached to counterparty paper. If it is attached to NBCU standard templates, certain definitions and sections may overlap. Please consult the NBCUniversal Privacy Playbook or the NBCU Privacy Legal Team for additional information.

1. Definitions.

1.1. Capitalized terms that are not defined have the meanings assigned to them in Applicable Law or the Agreement. In the event of conflict or inconsistency between this Addendum or the Agreement, this Addendum shall govern. References to "Service Provider" include its Personnel.

1.2. Defined terms used in this Addendum have the meanings set forth below.

"**this Addendum**" means this Data Processing Addendum, which forms part of the Agreement.

"Affiliate" of a party means any entity that (as of the Effective Date, or thereafter at the applicable time) directly or indirectly now or hereafter controls, is controlled by, or is under common control with that party.

"**Agreement**" means the *<insert name of main agreement, e.g. Master Services Agreement>* between *[insert names of parties to the main agreement]* with an Effective Date of *<insert date>*.

"**Applicable Law**" means all applicable laws, rules, regulations, rulings, judgments, directives, or other requirements of any governmental authority in any country or jurisdiction, as may be amended or otherwise revised from time to time and all applicable, current industry self-regulatory principles.

"**CCPA**" means the California Consumer Privacy Act as amended by the California Privacy Rights Act, and any related regulations.

"**Company**" means the NBCUniversal party to the Agreement.

"**Company Data"** means all data, including Company Personal Data, in any form, that is Processed by, or made available to, Service Provider or its Personnel in the course of providing Services under the Agreement, and all data regarding Company's use of the Services. Company Data includes Company's Confidential Information (which includes Company Personal Data, Company Content, and other Company Confidential Information) and any deliverables.

"**Company European Personal Data**" means all Company Personal Data to which Privacy Laws of the European Territories apply.

"Company Personal Data" means Personal Data that is Processed by or made available to, Service Provider in the course of providing Services under the Agreement.

"**Data Controller**", "**Data Processor**", "**Data Subject**", and "**Supervisory Authority**" shall have the meanings set out in the applicable Privacy Laws. Data Controller is inclusive of "**Business**" and "**Data Processor**" is inclusive of "**Service Provider**" as the terms are defined in the CCPA.

"**DPFs**" means collectively (i) the EU-U.S. Data Privacy Framework, (ii) the UK Extension to the EU-U.S. Data Privacy Framework, and (iii) the Swiss-US Data Privacy Framework.

"**Data Rights Request**" means a request by an individual to exercise their Privacy Law rights (regardless of whether the individual is actually entitled to that right).

"**European Territories**" means collectively (i) the European Economic Area ("**EEA**"), namely the European Union ("**EU**") Member States and Iceland, Liechtenstein and Norway, (ii) the United Kingdom ("**UK**") and (iii) Switzerland.

"**NBCUniversal Security Standard**" means the NBCUniversal Third Party Security Standard, the current version of which is set out in Appendix 2.

"**Order**" means a statement of work, order or other transactional document entered into by the parties pursuant to the Agreement.

"**Personal Data**" means any information that relates to an individual or household and that, alone or in combination with other information, can be used to identify, contact, or precisely locate an individual or household, or other information that constitutes "personal data" or "personal information" under Privacy Laws.

"**Personnel**" means, with respect to a party, that party's employees, Sub-processors, subcontractors, vendors, agents, officers, directors and other personnel.

"**Privacy Laws**" means all Applicable Laws and third-party platforms restrictions relating to the Processing of Company Personal Data, privacy and data security that may exist in any relevant jurisdiction.

"**Process**" (and any other tenses of the term "Process," such as "Processing") and words of similar nature mean using, accessing, storing, securing, sharing, disclosing, altering, destroying and deleting Personal Data and other actions as set forth in the applicable Privacy Laws.

"**SCCs**" means, in respect of Personal Data Processed by Service Provider for the benefit of NBCUniversal and/or its relevant Affiliates in: (a) the EEA and/or the Processing of EEA Personal Data, the unchanged, European Commission-approved version of the standard contractual clauses in Commission Decision 2021/914/EU (as set out in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en) (the "**EU SCCs**"); (b) the UK and/or the Processing of Company Personal Data to which Privacy Laws of the UK apply, the EU SCCs as modified by the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under s119A(1) of the Data Protection Act 2018 ("**UK SCCs**"); and (c) Switzerland and/or processing Personal Data to which the Swiss Federal Act on Data Protection of 25 September 2020 and its implementing regulations ("FADP") apply, a version of the EU SCCs that is deemed to be modified as follows: references to "Regulation (EU) 2016/679" shall be interpreted as references to the FADP; references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the FADP; references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", or "Swiss law" ("**Swiss SCCs**").

"Sell" (and any other tenses of the term "Sell" such as "Selling") means selling, renting, releasing, disclosing, disseminating, making available, transferring, licensing, sublicensing or otherwise communicating orally, in writing, or by electronic or other means, an individual's Personal Data to a third party for monetary or other valuable consideration.

"Sensitive Personal Data" shall have the meaning set out in the applicable Privacy Laws and shall include, but not be limited to, "special categories of personal data" (as defined in the Privacy Laws of the EEA and UK) and "sensitive personal information" (as defined in applicable US Privacy Laws), as applicable.

"**Service Provider**" means the entity providing the Services.

"**Services**" means the services provided to Company and/or its Affiliates under the Agreement and any Orders.

"**Share**" (and any other tenses of the term "Share," such as "Sharing") shall have the meaning set out in the applicable Privacy Laws.

"**Sub-processor**" means any external party, including Service Provider's Affiliates and subcontractors, appointed by Service Provider to Process Company Personal Data. References to a Sub-processor include its Personnel.

"**Systems**" means 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.

"**Third Country**" means, (i) if the relevant Company entity is established in the EEA or Switzerland, a jurisdiction outside the EEA or Switzerland that has not been deemed adequate for data protection purposes by the European Commission, or (ii) if the relevant Company entity is established in the UK, a jurisdiction outside the UK that has not been deemed adequate for data protection purposes under UK law.

2. Roles and Responsibilities of the Parties.

2.1. Independent Controllers. Each Party ("**Controller Party**") acknowledges that it is an independent data controller with respect to Business Contact Data. "**Business Contact Data**" is Personal Data of the other Party's Personnel Processed by Controller Party for the purpose of facilitating the Services and maintaining the business relationship with the other Party. Each Party represents and warrants that it shall limit the use of Business Contact Data to such purposes.

2.2. Service Provider as Data Processor. The parties acknowledge that Company or its relevant Affiliates act as the Data Controller of the Company Personal Data Processed by Service Provider in its provision of the Services, and Service Provider acts as the Data Processor of such Company Personal Data. Service Provider acknowledges and agrees that between Service Provider and Company, Company owns all Company Data. In the event Company or its relevant Affiliates act as a Data Processor and Service Provider acts as the sub-processor, (a) each reference to Company or its Affiliates in their capacity as a Data Controller shall be interpreted to include the applicable Data Controller and (b) each reference to Service Provider as a Data Processor shall be interpreted to mean Service Provider's role as a sub-processor.

3. Processing and Disclosure of Company Personal Data.

3.1. Purpose of Processing Company Personal Data. Service Provider shall only Process Company Personal Data in accordance with Company's written instructions and the Processing Overview in Appendix 1 of this Addendum, unless Service Provider is otherwise required by Applicable Law, in which case Service Provider shall (if legally possible) inform Company of that requirement before Processing the Company Personal Data. Company instructs Service Provider to Process Company Personal Data only to the extent necessary to perform the Services in accordance with the Agreement, this Addendum and the relevant Order. Service Provider shall notify Company immediately if it reasonably believes that any instruction given by Company is contrary to Privacy Law. Service Provider shall inform Company if it makes a determination that it cannot meet the requirements of this Addendum or a Privacy Law.

3.2. Restrictions on Processing. Service Provider shall not, without Company's prior written consent: (a) Process Company Personal Data for any independent purposes including outside the direct relationship with the parties, any purposes that are unrelated to providing the Services, or for the commercial benefit of Service Provider or any of Service Provider's other clients (to the extent permitted under Privacy Laws, detecting data security incidents, exercising and defending claims, and protecting against fraudulent or illegal activity are not considered commercial benefits); (b) Sell or Share Company Personal Data; (c) to the extent Company Personal Data is anonymized or pseudonymized, re-identify, or attempt to do so with, such Company Personal Data, or any portions thereof; (d) delete or modify any Company Personal Data; (e) disclose Company Personal Data or any related summaries or reports to any third party or allow any third party to access it, including disclosure in any manner that would identify the methods, scope or scale of Company Personal Data or Company's use of the Services; or (f) combine Company Personal Data with or match Company Personal Data to Personal Data from its own or third parties' interactions with an individual. Service Provider certifies that it understands and will comply with the restrictions set forth in this Section 3. Service Provider shall comply with the obligations of the CCPA and provide at least the same level of privacy protection as required by the CCPA. Company shall have the right to take reasonable and appropriate steps to help ensure that Service Provider uses the Company Personal Data in a manner consistent with Company's obligations under Privacy Laws. Company shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate the unauthorized use of Company Personal Data. If Company directs Service Provider to cease or limit processing of Sensitive Personal Data Processed by Service Provider on behalf of Company, then it shall promptly do so, and cause its Personnel to do the same.

3.3. Required Disclosures. If Service Provider is required by Applicable Law to grant access to or otherwise transfer Company Personal Data to a third party (whether nationally or internationally), it shall:

(a) redirect the third party to request such information directly from Company;

(b) if permitted by Applicable Law, give Company as much prior notice as is reasonably possible;

(c) limit such access or transfer to the minimum required by Applicable Law; and

(d) provide Company with all reasonable assistance should Company choose to challenge such access or transfer.

3.4. Processing Overview. The categories of Company Personal Data to be Processed, the Processing activities to be performed, and the Sub-processors and Processing locations are set out in Appendix 1 to this Addendum or the relevant Order.

3.5. Data Processing Obligations. Service Provider shall at no additional cost to Company:

(a) ensure that its Personnel are only granted access to Company Personal Data on a need-to-know basis; are bound by appropriate obligations of confidentiality; are appropriately supervised; and are provided with appropriate training in the care and handling of Company Personal Data;

(b) provide such information, cooperation and assistance to Company as Company may reasonably require to allow Company and its Affiliates to comply with their obligations under Privacy Laws including documentation needed to (i) demonstrate Service Provider's compliance with this Addendum; (ii) facilitate data protection impact assessments, (iii) address any enquiry, notice or investigation by a governmental authority, and (iv) facilitate the collection of required consents from data subjects;

(c) maintain written records of all categories of Processing activities carried out on behalf of Company containing the information prescribed in applicable Privacy Laws, and make such records available to Company on request; and

(d) notify Company promptly (and in any event within 2 business days) if Service Provider or its Personnel receive any inquiry or notice (including notice of investigation) from a governmental authority in relation to the Services provided under the Agreement.

3.6. Data Rights Requests. Service Provider will promptly (and in any event within 2 days' of Company's request) provide all information, co-operation or assistance as Company may reasonably require to fulfill the Data Rights Request. In addition, Service Provider will promptly inform Company of any Data Rights Requests regarding Company Personal Data that it receives directly from or on behalf of an individual. Service Provider shall either (a) provide an industry standard integration mechanism for the fulfillment of Data Rights Requests, or (b) integrate with a Data Rights Request fulfillment mechanism reasonably specified by Company.

3.7. Sub-processors. Service Provider is permitted to utilize the Sub-processors listed in Appendix 1 to process Company Personal Data, and is permitted to appoint additional or replacement Sub-processors to process Company Personal Data, subject in all cases to Service Provider:

(a) carrying out adequate due diligence and monitoring to ensure that the Sub-processor will provide the level of protection for Company Personal Data that is required under this Addendum and, if applicable, the SCCs;

(b) providing at least 30 days' notice to Company of the identity and location of the proposed Sub-processor, a description of the intended processing to be carried out by the Sub-processor, the proposed data transfer mechanism (if applicable), and confirmation that adequate due diligence has been conducted on it, in order to give Company the opportunity to consider and object to such changes prior to the use of the proposed Sub-processor;

(c) complying with the requirements of Section 4.2(b) (Onward Transfers) and Section 4.3 (Transfers of Bulk U.S. Sensitive Personal Data) below; and

(d) requiring each of its permitted Sub-processors that Process Company Personal Data to enter into an agreement that imposes the same or substantially similar obligations that are in this Addendum.

If Service Provider identifies deficiencies in a Sub-processor's privacy or security controls, Service Provider shall maintain a record of such findings and ensure that such deficiencies are remediated within appropriate timeframes. Service Provider is liable to Company for the failure of Service Provider Personnel to comply with the Agreement to the same extent that Service Provider would have been had Service Provider failed to comply.

3.8. Data Return and Deletion. Unless (i) otherwise requested by Company in writing, or (ii) Service Provider is required to retain it 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 Personal Data in the possession, custody or control of Service Provider, at the earlier of conclusion of the applicable Services, upon Service Provider no longer needing to Process Company Personal Data to provide the Services, or on written instruction from Company, and shall direct its Sub-processors to do the same. Service Provider shall promptly on Company's request certify that such Company Personal Data has been returned, deleted or destroyed.

4. Cross Border Data Transfer.

4.1. Compliance with Cross-Border Data Transfer Requirements. Service Provider shall, and shall ensure that its Sub-processors shall, comply with (and cooperate with Company to facilitate Company's and its Affiliates' compliance with) the requirements of applicable Privacy Laws, related to cross-border data transfer and/or data localization, such as the execution of data transfer agreements with Company or its Affiliates. If, for whatever reason, the transfer of Company Personal Data to Service Provider ceases to be lawful, the parties will work together in good faith to put in place alternative or supplementary measures to enable the compliant receipt of the Services. If Company and Service Provider are unable to agree on suitable measures to address the issue, then Company may (at its option) terminate the Agreement or reduce its scope.

4.2. Transfers of Company Personal Data.

(a) **SCCs.** If Service Provider (i) is established in a Third Country and Processes Company European Personal Data, or (ii) Processes Company European Personal Data at or from its facilities in a Third Country, the SCCs shall be incorporated by reference in this Addendum and shall apply between Company (and/or its relevant Affiliates in the European Territories), and Service Provider. The Appendix to this Addendum (as may be varied for a particular Order by the insertion of replacement information concerning the Processing) sets out the parties' roles and the information required by the Annexes to the SCCs. Nothing in this Addendum shall be construed to prevail over any conflicting clause of the SCCs. Each party acknowledges that it has had the opportunity to review the SCCs.

(b) **Onward Transfers.** Service Provider may transfer Company Personal Data to a third party or a location outside the country of origin, provided that Service Provider complies with the requirements of applicable Privacy Laws, including (where appropriate): transferring the data to a territory which has been approved as providing adequate protection under applicable Privacy Laws, participating in a valid cross-border data transfer mechanism under applicable Privacy Laws so as to provide appropriate safeguards for such data (e.g. the use of standard contractual clauses or binding corporate rules), and taking other steps required under applicable Privacy Laws such as performing third country risk assessments and applying supplementary measures to protect the data.

(c) **Data Privacy Frameworks.** "**DPF Certifications**" means self-certifications made by an eligible US company under each of the DPFs. If the parties wish to rely on Service Provider's DPF Certifications as a data transfer mechanism in place of the SCCs, Part 3 of Appendix 1 will be completed accordingly. Company's acceptance of Service Provider's DPF Certifications in place of SCCs is made in reliance on the representations and warranties in Section 4.2(d), and is subject to the provisions of Section 4.2(e).

(d) **DPF Representations and Warranties.** Service Provider hereby represents and warrants that: (i) Part 3 of Appendix 1 accurately reflects its DPF Certifications; (ii) Service Provider has not taken steps to voluntarily withdraw from any of these frameworks; and (iii) the scope of each of the self-certifications covers the services and processing activities that will be undertaken by Service Provider under this Agreement.

(e) **Use of SCCs if the DPFs are not a sufficient data transfer mechanism.** If (i) Service Provider ceases to hold a DPF Certification that Company or any of its Affiliates requires as a data transfer mechanism, or (ii) the scope of any of Service Provider's DPF Certifications ceases to cover the services and processing activities that are undertaken by Service Provider under this Agreement; or (iii) any of the DPF Certifications becomes invalid as a data transfer mechanism, the parties agree that the SCCs will be incorporated by reference into this Addendum in accordance with Section 4.2(a) above, and will be deemed to have been executed by the parties as at the date of the relevant event listed in this section.

4.3. Transfers of Bulk U.S. Sensitive Personal Data. Service Provider represents and warrants that Service Provider is not a Covered Person or Country of Concern, as set forth in Section 202.302 of the Department of Justice Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, as amended from time to time (the "**DOJ Rule**") and will immediately notify Company if it foresees any circumstance or situation that would cause it to become such a Covered Person or Country of Concern. Service Provider shall not, without prior written consent from Company, transfer, disclose, sell, resell, sublicense, or otherwise permit access to any bulk U.S. sensitive personal data to: (a) any individual or entity located in a Country of Concern; (b) any Covered Person; or (c) any third party that intends to, or is likely to, transfer the data to a Country of Concern or a Covered Person. All terms in this section have the definitions assigned to them under the DOJ Rule.

5. Data Security

5.1. Security. To protect Company Data, Service Provider shall (a) implement and maintain administrative, technical, physical, operational and organizational safeguards regarding security, continuation, backup, and disaster-recovery that are consistent with then-current, highest industry standards and practices and comply with Applicable Law; (b) only access and use Company Systems to the extent necessary to perform the Services; and (c) comply with the NBCUniversal Security Standard, which Company may from time to time update and modify upon written notice to Service Provider. Service Provider shall regularly review the security measures it has implemented to protect Company Personal Data so as to ensure their appropriateness with regard to risk to the rights and freedoms of natural persons, which may evolve over time.

5.2. Security Incident. A "**Security Incident**" is any accidental, unlawful, or unauthorized access, use, damage, destruction, alteration, loss, or disclosure of Company Data (including by or on behalf of Service Provider or its Personnel, or by or through any of their Systems or the Services or deliverables). Service Provider will notify Company without undue delay and in any event within 48 hours (and otherwise in accordance with the NBCUniversal Security Standard) of becoming aware of any Security Incident. 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 the Security Incident (including the categories and approximate number of Data Subjects 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 its 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. Service Provider must send notifications of Security Incidents to its main contact under the relevant Order, with a copy to cyber@nbcuni.com.

5.3. Communications. Company reserves the right to manage all communications concerning Company's or its Affiliates' involvement in any Security Incident with the affected individuals, governmental entities, the public and/or third parties. Service Provider shall not issue, publish or make available to any third party any statement, press release or any other communication that mentions Company or its Affiliates and concerns the Security Incident without Company's prior written approval. The foregoing provisions are not intended to restrict Service Provider's ability to communicate with its other customers or make legally required communications or notifications.

6. Data Protection Audits and Reviews.

6.1. Company shall have the right to audit Service Provider. Service Provider shall cooperate and provide accurate information. Company or its representatives may conduct such audits annually. If required by Applicable Law or if a Security Incident occurs, Company may conduct additional audits. The audits may include onsite visits. Service Provider shall permit Company to carry out ongoing manual reviews and automated scans for the purpose of monitoring Service Provider's compliance with this Addendum. If as a

result of audits or reviews described in this Addendum, Company determines that Service Provider has failed to perform any of its obligations under this Addendum and/or the Agreement, then Service Provider shall, within ten (10) days develop a corrective action plan (including timeline), subject to Company's approval, and shall implement this plan accordingly. Service Provider shall certify in writing to Company that the corrective action plan has been completed upon request.

7. Miscellaneous

7.1. Service Provider shall:

(a) comply with all Privacy Laws in performing the Services and its other obligations under the Agreement;

(b) obtain all registrations and consents, and pay all fees, required by Privacy Laws for Service Provider's performance and/or Company's receipt of the Services and deliverables; and

(c) cause its Personnel working on Company's premises, or having access to Company Systems, to comply with all applicable Company regulations and policies. Service Provider shall take reasonable precautions with respect to the employment of and access given to its Personnel, including conducting background checks.

7.2. Materiality and Injunction. Without limitation to any other remedies, Company shall be entitled to seek equitable relief for any breach of this Addendum without posting any bond. Service Provider acknowledges that any breach by Service Provider of this Addendum constitutes a material breach of the Agreement.

8. Indemnification **[**Add language located in the NBCUniversal Privacy Toolkit if there are no adequate indemnification provisions in another agreement with the Service Provider that would cover NBCU for breaches under this DPA**].**

Appendix 1 to Data Processing Addendum

DRAFTING NOTE: *This Appendix contains the information needed for the proper incorporation of the EU, UK and Swiss SCCs It also contains the Processing Overview that is needed for all US/UK/EEA/Swiss contracts. If the deal is US-only, or if the Service Provider is based in the EEA, UK or a country whose data laws are considered "adequate" (check these lists: EU list / UK list), there is no need to incorporate the SCCs, and you can just complete Part 2B (Processing Overview), or use the DPA (US-only) or DPA (International) template as appropriate.*

Part 1: Information required by SCCs. Note: All references to Clauses and Annexes below are to the Clauses and Annexes of the SCCs.

1. **EU SCCs, Swiss SCCs and UK SCCs:** The parties' roles (as data exporter or data importer; Data Controller, Data Processor or sub-processor) shall be as specified in Part 2A below, and the relevant Modules of the SCCs shall apply depending on those roles.

2. Part 2 of this Appendix 1 shall be deemed to be Annex I of the EU SCCs, Swiss SCCs and UK SCCs, and Appendix 2 to this Addendum shall be deemed to be Annex II of the EU SCCs, Swiss SCCs and UK SCCs.

3. **EU SCCs, Swiss SCCs and UK SCCs:** In Clause 9(a) (Use of sub-processors), Option 2 (General Written Authorisation) shall apply, and the time period for informing the data exporter of intended changes to the list of sub-processors shall be 30 days.

4. **EU SCCs, Swiss SCCs and UK SCCs:** The optional wording in Clause 11 (Redress) shall not apply.

5. **UK SCCs:** For the purpose of Section 19 of the UK SCCs, neither party shall have the right to end the UK SCCs when a revised version is issued by the Information Commissioner's Office.

6. **Governing law and Jurisdiction:** The following option and choice of law shall apply in the following scenarios:

Data exporter	**SCCs Clause 17 – Governing Law**	**SCCs Clause 18 – Choice of forum and jurisdiction**
Company and its US, EEA and Swiss affiliates that have signed an Order	Option 1 – the laws of the Netherlands	The courts of Amsterdam in the Netherlands

7. **Swiss SCCs:** Clause 18(c) of the EU SCCs provides that "A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence." For the purpose of the Swiss SCCs, the reference to "the Member State in which he/she has his/her habitual residence" in this clause shall be deemed to be a reference to "Switzerland".

Part 2: Processing Overview / Annex I of the SCC

A. LIST OF PARTIES

Details of data exporters

Name	Address	Contact person's name address and contact details	Activities relevant to the data transferred under these clauses	Role
[NBCUniversal Media, LLC – *this entity should match the entity that is entering into the MSA*] ("NBCUniversal")	30 Rockefeller Plaza New York NY 10112 USA	Chief Privacy Officer Privacy Legal Department NBCUniversal 30 Rockefeller Plaza, New York, NY 10112, USA **EU Representative:** Privacy Legal Department Universal Studios International B.V. Moermanskkade 421 1013 BC Amsterdam, The Netherlands **UK Representative:** Privacy Legal Department NBCUniversal International Limited 1 Central St Giles, St Giles High Street, London WC2H 8NU, United Kingdom	The data exporter is a US-based media and entertainment company that is contracting with data importer for it to provide services to the data exporter for itself and for the benefit of its affiliates.	Controller
UK, EEA and Swiss affiliates of NBCUniversal that have placed Orders with Service Provider	c/o NBCUniversal International Ltd, 1 Central St. Giles St. Giles High Street London WC2H 8NU United Kingdom	Privacy Legal Department, Chief Privacy Officer c/o NBCUniversal International Ltd 1 Central St. Giles St. Giles High Street London WC2H 8NU United Kingdom	The data exporters are part of the same media and entertainment group as the data exporter named above, and will be procuring services from the data importer pursuant to the contract mentioned above.	Controller

Details of data importer

Name	Address	Contact person's name address and contact details	Activities relevant to the data transferred under these clauses	Role
[Service Provider to complete]	[Service Provider to complete]	[Service Provider to complete]	The data importer is a [*US-based*] provider of [*specify*] solutions	Processor

B. DESCRIPTION OF TRANSFER / PROCESSING OVERVIEW

1. Categories of data subjects whose Personal Data is Processed or transferred

Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organization, it includes their staff.

- Business contacts
- Consumers/General Public
- Contractors and Employees
- [INSERT ADDITIONAL CATEGORIES IF APPLICABLE]

2. Categories of Personal Data Processed or transferred

- Contact Information, e.g. email address, telephone number, address
- Device information and identifiers, e.g. IP address, cookie IDs, device type, advertising and app identifiers
- [INSERT ADDITIONAL CATEGORIES IF APPLICABLE]

3. Categories of Sensitive Personal Data Processed or transferred

The Personal Data transferred concern the following special categories of data (please specify):

[***DRAFTING NOTE***: *Either insert "None", or insert the relevant categories of sensitive Personal Data from the first list below, as well as the relevant additional safeguards from the second list:*

[None] or

[If and to the extent required to be processed in order to provide the Services under the Agreement, Personal Data revealing [racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation – *delete as appropriate*].

The following restrictions and/or safeguards are applied:

- [strict purpose limitation,
- access restrictions (including access only for staff having followed specialized training),
- keeping a record of access to the data,
- restrictions for onward transfers
- additional security measures. – *delete as appropriate*]]

4. **The frequency of the transfer**

The data is transferred on a [continuous] / [one-off] basis. ***[DRAFTING NOTE:** Delete as appropriate]*

5. **Nature of the Processing**

The Personal Data transferred will be subject to the following processing activities (please specify):

[***DRAFTING NOTE**: Describe the type of processing. Adapt the sample below as appropriate. Make sure that this section clearly describes the specific business purposes for which the Service Provider is authorized to process the personal data.*]

[In order to provide the Services described in this Agreement and any Order, Service Provider will [host, maintain and support a system Processing Company Personal Data – *Note: This is sample language – adapt this as appropriate to describe the processing activities.]*. Service Provider will grant NBCUniversal's authorized users electronic access to this system.]

6. **Purpose of the transfer and further Processing**

The purpose of the transfer and Processing is as described in paragraph 5 above (Nature of the Processing).

7. **Period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period**

The data importer will retain the Personal Data for the duration of its agreement with the data exporter or as otherwise specified in the Agreement, unless instructed by data exporter to return or delete such Personal Data at an earlier or later date.

8. **Permitted Sub-processors**

	Sub-processor	**Subject matter and nature of processing**	**Country in which the sub-processing will take place and applicable data transfer mechanism (e.g. SCCs, DPF, BCR)**	**Duration of processing**
1.	[to be completed by Service Provider – insert full legal name of sub-processor, including affiliates.]	[to be completed by Service Provider – e.g. data hosting; customer services helpdesk; software maintenance and support services; fulfilment services]	[Service Provider to complete, e.g. USA – DPF, or USA - SCCs]	Sub-processor will process the personal data for the duration of its agreement with the data importer, unless instructed by data importer or data exporter to return or delete the data at an earlier or later date.
2.				

C. COMPETENT SUPERVISORY AUTHORITY

The following paragraphs of Clause 13(a) of the SCCs shall apply:

"Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of the GDPR is established, as indicated in Annex I.C, shall act as competent supervisory authority."

For the purpose of the SCCs being entered into for the benefit of NBCUniversal Affiliates in Switzerland, the reference to "an EU Member State" in Clause 13(a) shall be deemed to be a reference to "Switzerland".

Data exporter	**Competent supervisory authority**
NBCUniversal and its US Affiliates	The Dutch Data Protection Authority (Autoriteit Persoonsgegevens)
NBCUniversal's EEA and Swiss affiliates	The supervisory authority for the country in which the relevant affiliate is located

Part 3: Service Provider's DPF Certifications

Name of Certification	**Service Provider to insert "X" to confirm that it has an active self-certification covering the Services**
EU-US Data Privacy Framework	
UK Extension to EU-US Data Privacy Framework	
Swiss-US DPF	

Appendix 2 to the Data Processing Addendum
Technical and Organisational Measures to Ensure the Security of the Data
NBCUniversal Third Party Security Standard

NBCUniversal Third Party Security Standard	Effective Date: 19 Dec 2025
	Version No.: 7.0

Contents

1. Introduction

NBCUniversal recognizes information protection and protection of Intellectual Property requires close cooperation between NBCUniversal 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 **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 Company Level 3 Confidential and Level 4 Sensitive Non-Public 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.

4.5.6 **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 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 Science 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**

Has the same meaning as 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.

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	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,	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	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.

Data Class Name			Cyber Sensitive Information		
	control access to Non-Business Information.		organizational assets, or individuals.	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 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 Tier 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
Mei-lan Stark, Executive Vice President and Chief Counsel, Intellectual Property

Approval Date: 10 December 2025
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

Version	Changes	Approved	Published	Effective
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 *Executive Summary for Third Party Security Standard v 6.0.* • Incorporated requirements form 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
6.1	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