DATED 15 September 2023

SKY CP LIMITED

AND

SPREEDLY, INC.

AMENDMENT TO SPECIAL TERMS AND CONDITIONS DATED 15 OCTOBER 2019

THIS AMENDMENT AGREEMENT ("AMENDMENT") is made on 15 September 2023

BETWEEN:

(i) **SKY CP LIMITED** (company number 09513259) whose registered office is at Grant Way, Isleworth, Middlesex, TW7 5QD ("**Sky**"); and

(ii) **SPREEDLY, INC.** whose registered office is at 300 Morris Street, Suite 400 Durham, NC 27701 ("**Supplier**"),

(each "**Party**" and together the "**Parties**").

WHEREAS:

(A) Sky and Supplier agreed to Special Terms and Conditions dated 15 October 2019 ("**Special Terms**") which incorporated, subject to variations in the Special Terms, Sky's Standard Terms and Conditions for the Purchase of Goods, Licenses and Services (as amended from time to time including by the Notice of Changes to Standard Contractual Clauses dated 3 November 2022 and Amendment to Special Terms and Conditions with an effective date of 28 November 2022) ("**Terms and Conditions**") and Orders #1 and #2 in Schedule 2 of the Special Terms. The Special Terms, together with the Terms and Conditions and Orders #1 and #2 constitute the "**Agreement**"; and

(B) Sky and Supplier now wish to amend the Agreement as set out in section 1 below with effect from the last date of signature by a Party in the signature block below ("**Amendment Effective Date**").

IT IS AGREED:

1. For good and valuable consideration, receipt of which is hereby acknowledged as received, the Parties agree to vary the Agreement with effect from the Amendment Effective Date as follows:

1.1. In clause 1 (Definitions) of the Special Terms, the definition of 'Sky Affiliate' is hereby deleted in its entirety and replaced with the following:

> **Sky Affiliate**: means, with respect to Sky, any other entity directly or indirectly Controlling or Controlled by, or under direct or indirect common Control with, Sky or one or more of the other affiliates of that entity (or a combination thereof), as of the Effective Date or thereafter;

1.2. In clause 1 (Definitions) of the Special Terms, the definition of 'Sky Joint Venture' is hereby deleted in its entirety and replaced with the following:

> **Sky Joint Venture:** means any joint venture entity to whom Sky or a Sky Affiliate provides technical, infrastructure or enterprise services as part of such joint venture and any entity Controlled by such joint venture;

1.3. In clause 1 (Definitions) of the Special Terms, a new defined term, 'Control', is hereby added as follows:

> **Control:** means 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 or otherwise. With respect to Sky Group Party only, "ownership" means direct or indirect ownership of at least 20% of voting securities, equity interest or the equivalent;

1.6. 1.5 In clause 1 (Definitions) of the Special Terms, the term 'Service' shall be deemed to include the term 'Deliverable'. Schedule 7 of the Special Terms is hereby deleted in its entirety and replaced with a new Schedule 7 as set out in Annex 1 of this Amendment.

1.7. In Schedule 7 of the Special Terms, the following new sub-paragraph is added to paragraph 14:

14.16 The Sky Group may, from time to time, restructure, sell or transfer any Sky Group entity or a department or division within one or more Sky Group entity (each a "Divestment"), with the sold, transferred or restructured Sky Group entity, or department or division, becoming a "Divested Business". Supplier acknowledges and agrees that Sky may elect to grant to any Divested Business a right to use and/benefit from the Deliverables under the Agreement, at no additional charge as if such Divested Business were still a Sky Group entity, which right may continue for up to 36 months following the effective date of the relevant Divestment provided that Sky shall ensure that such Divested Business complies with the terms of the Agreement as contemplated in clause 10.6.

1.8. Schedule 6 (Security and Privacy Addendum) of the Special Terms of the Agreement shall be revised as set forth below.

1.8.1. The defined terms "**data controller**", "**data processor**", "**data subject**", "**process/processing**", and "**supervisory authority**" set forth in Section 1.1. of Schedule 6 of the Special Terms shall be deleted and replaced in its entirety with the following:

The terms "**data controller**", "**data processor**", "**data subject**", "**process/processing**", and "**supervisory authority**" shall be deemed to have the meanings (or reasonably equivalent meanings) set out in the applicable Privacy Laws, except that, to the extent applicable, data controller shall be inclusive of "**business**" and "**data processor**" is inclusive of "**service provider**" as the terms are defined in the California Consumer Privacy Act ("**CPRA**");

1.8.2. The defined term "**Sky Systems**" set forth in Section 1.1. of Schedule 6 of the Special Terms shall be deleted and replaced in its entirety with the following:

"**Sky Systems**" means Systems owned or controlled by Sky, Sky Joint Ventures, or Sky Affiliates, or their Personnel (for clarity, not including Spreedly or its Personnel).

1.8.3. **Restrictions on Processing and CPRA.** The following shall be added to Section 2.2:

(1) Spreedly may not, without Sky's prior written consent: process Sky 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 for purposes of this provision) (i) sell or share (as such terms are defined in applicable Privacy Laws) Sky Personal Data; or (ii) combine Sky Personal Data with or match Sky Personal Data to Personal Data from its own or third parties' interactions with an individual.

(2) Spreedly shall comply with the obligations of CPRA and provide at least the same level of privacy protection as required by CPRA. Sky shall have the right to take reasonable and appropriate steps to help ensure that Spreedly uses the Sky Personal Data in a manner consistent with Sky's obligations under Privacy Laws. Sky shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate the unauthorized use of Sky Personal Data. If Sky directs Spreedly to cease or limit processing of sensitive information (as defined by Privacy Law) provided by Sky or its Affiliates to Spreedly, then it shall promptly do so, and cause its Personnel to do the same. Spreedly shall inform Sky if it makes a determination that it cannot meet the requirements of the data privacy and security obligations set forth in this Agreement or a Privacy Law. Spreedly shall regularly review the security measures it has implemented to protect Sky 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.

1.8.4. **Notifications of Requests and Inquiries.** Section 2.10 shall be deleted and replaced in its entirety with the following:

(a) Spreedly will promptly notify Sky of any enquiry, notice or investigation by a regulatory or supervisory authority received by Spreedly, in each case where such contact arises in connection with the Services provided under this Agreement.

(b) "**Data Rights Request**" means a request by an individual to exercise his or her Privacy Law rights (regardless of whether the individual is actually entitled to that right). Spreedly will promptly (and in any event within business 2 days of Company's request) provide all information, co-operation or assistance as Sky may reasonably require to fulfil the Data Rights Request. In addition, Spreedly will (A) integrate with any technical solution required by Sky for the purpose of transmitting and honoring Data Rights Requests, including third party APIs or other services, as directed by Sky and (B) promptly inform Sky of any Data Rights Requests regarding Sky Personal Data that it receives directly from an individual. With respect to (A), if Company requires any changes to the Services or Spreedly systems or operations that are (1) not de minimis, (2) different from the Services, systems and operations in effect as of the Amendment Effective Date and (3) exceed then-current industry standards for vendors that Process Personal Data, then Sky acknowledges that such changes may be at Sky's expense, provided that any additional fees are agreed in a signed Order.

1.8.5. **Processor-Processor Relationship**. Notwithstanding the final sentence of Sentence 3.1, Sky and/or its relevant Affiliates act as the Data Controller or Data Processor (acting on the instructions of the applicable Data Controller) of the Sky Personal Data Processed by Service Provider in its provision of the Services, and Service Provider acts as the Data

Processor (or, if applicable, the "sub-processor" under applicable Privacy Laws) of such Sky Personal Data.

1.8.6. **Scans**. The following shall be added to Section 3.4:

In addition to the audit and inspection rights described in the Agreement, Spreedly shall permit Sky to carry out ongoing manual reviews and automated scans for the purpose of monitoring Spreedly's compliance with this Privacy Addendum.

1.8.7. **No Penetration Testing without Consent**. Notwithstanding the final sentence in 4.1 of the NBCUniversal Third Party Information Security Standard, Sky shall not, without prior written consent of Spreedly, conduct penetration testing of Spreedly's and its Personnel's Systems that may adversely affect Spreedly's Services. Upon Sky's request, Spreedly will provide a summary (including all material findings) of the results of penetration testing of Spreedly's and its Personnel's Systems and the Services conducted by a qualified third party and relevant reports.

1.8.8. **Technology Security Standards.** The following provisions are hereby added to Part 1: NBCUniversal Third Party Information Security Standard of Annex 3 to Privacy Addendum to Schedule 6 of the Special Terms:

Access Controls

1. Spreedly shall implement Modern Authentication and Multi Factor Authentication (MFA) for any application, software, or system that accesses, transmits, receives, collects, generates, uses, stores, processes, or shares NBCUniversal Data, Sky Group Business Information or Content.

2. "Multifactor Authentication (MFA)" means authentication that requires more than one distinct authentication factor for successful authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors.

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

Individual Contractor Requirements

1. Contractor Obligation. Without limitation, any violation is a material breach of the Agreement and NBCUniversal reserves the right to terminate the Agreement and/or remove the Individual Contractor(s) supporting NBCUniversal on behalf of Spreedly, immediately upon breach of any of these requirements.

2. NBCUniversal Cyber Security Policies and Standards. Individual Contractors must adhere to the NBCUniversal cyber

security policies and standards at Schedule 11. Spreedly must inform their Individual Contractors about the cyber security policies and standards and their obligation to adhere.

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

4. Security Incident Reporting. For any Security Incident involving NBCUniversal administered systems, and without limitation to any Spreedly obligations with respect to notices of Security Incidents, Individual Contractors must immediately report a Security Incident via email to cyber@nbcuni.com or via phone to the 24-Hour Incident Hotline at +1-855-650-SAFE (7233).

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

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

7. Misuse of NBCUniversal Internet. Individual Contractors must not misuse NBCUniversal Internet. The Acceptable Use Policy is in the cyber policy library, and can be accessed at any time while connected to the NBCUniversal Intranet.

8. Phishing Program. For Individual Contractors, if any, that are provided NBCUniversal email addresses: Individual Contractors must successfully pass the simulated phishing training program. All Individual Contractors are expected to be able to identify a simulated or real phishing email and must report phishing emails to NBCUniversal Cyber Security. Individuals successfully pass a simulated phishing campaign if they correctly identify the simulated

phishing email and report it to cyber@nbcuni.com without clicking on the simulated link, opening the simulated attachment, or entering their credentials on the simulated site. Immediate education is provided to all who take prohibited actions with respect to phishing emails. Without limitation, repeated failure to pass a simulated phishing campaign, including the taking of prohibited actions with respect to phishing emails, shall be deemed a material breach of the Agreement.

For purposes of the foregoing, the term "Individual Contractor" means individuals that are Personnel of Spreedly that are granted access privileges to any systems owned, controlled or licensed by Sky or its Affiliates.

1.14 **Export Control.**

1.14.1 The following shall be inserted into the Agreement as a new Section 3.10:

3.11 Export Control. Service Provider will comply with the obligations in Schedule 10.

1.14.2 Schedule 10 is hereby added to the Agreement as is attached hereto as Annex 2.

1.15 **Additional NBCUniversal Security Standards**. Schedule 11 is hereby added to the Agreement as attached hereto as Annex 3.

2 Except to the extent expressly amended by this Amendment, defined terms and words in the Agreement shall have the same meaning when used in this Amendment.

3 Except for the provisions expressly set forth in this Amendment all provisions of the Agreement shall remain unchanged.

4 This Amendment shall be without prejudice to any right or remedy which may have accrued to either Party prior to this Amendment.

5 This Amendment shall be governed by and construed in accordance with the laws of England and any dispute or claim arising out of or in connection with this Amendment which the Parties cannot settle will be subject to the exclusive jurisdiction of the English Courts.

Signed for and on behalf of

SKY CP LIMITED

Name: Rhys Jones

Position: Director, OTT Products

Date: 15 September 2023

Signed for and on behalf of

SPREEDLY, INC.

Name: Nellie Vail

Position: CFO

Date: 14 September 2023

ANNEX 1
SCHEDULE 7
TERMS & CONDITIONS

Sky Standard Terms
(05.01.2023) v60(632

ANNEX 2

SCHEDULE 10

EXPORT CONTROL

1. Spreedly shall (i) on an ongoing basis throughout the term of the Agreement and (ii) upon final delivery and acceptance of any Services:

1.1. provide Sky with sufficient information regarding levels of encryption technology in, and ECC-N classifications applicable to, the Services (including changes thereto) for Sky to comply with all applicable export and import law and regulations;

1.2. ensure that all Personnel of Spreedly performing Services within the United States and using or accessing software or technology whose export is restricted by Export Controls are US citizens, permanent resident aliens or aliens otherwise authorized to be employed in the US under Applicable Law.

2. Spreedly represents, warrants and agrees that neither Spreedly nor any of its subsidiaries, directors, officers or controllers is the subject of any embargoes, sanctions, trade controls, or investment restrictions imposed, administered, or enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), the U.S. Commerce Department, the U.S. State Department, Executive Orders by the President of the United States, the United Nations Security Council, the United Kingdom, the European Union or any member thereof (collectively, "**Sanctions**") and that all Services provided hereunder shall be in compliance with all applicable Sanctions and export control laws, including those administered by the US Department of Commerce Bureau of Industry and Security and the US State Department Directorate of Defense Trade Controls ("**Export Controls**"). Any breach of the foregoing representations, warranties and agreements during the applicable Subscription Term shall entitle Sky to immediately suspend the rights and obligations of both Parties hereunder and to terminate this Agreement upon five (5) days written notice. Spreedly shall notify Sky in writing no later than one (1) business day following the date on which any of Spreedly or any of Spreedly's subsidiaries, directors or officers becomes the subject of Sanctions.

3. If Sky determines in its sole discretion that performing, or failing to perform, one or more of its obligations under this Agreement would be contrary to or required by any Sanctions or Export Controls, Sky's performance of, or failure to perform, such actions shall not constitute a breach of this Agreement by Sky and Sky shall not be liable to Spreedly, or any third party, for any damages arising as a result of Sky's performance of, or failure to perform, such obligations.

ANNEX 3

SCHEDULE 11

ADDITIONAL POLICIES

See attached.

NBCUniversal	**Title:**	NBCUniversal Acceptable Use Policy	
	Division:	Operations & Technology	
	Owner:	Technical Operations	
	Effective: 06/05/2023	**Last Update:** 06/05/2023	Page 1 of 5

NBCUniversal Acceptable Use Policy

1. Acceptable Use Policy

The Acceptable Use Policy ('**Policy**') reflects the Company's global standards for accessing, creating, and sharing of electronic information for or on behalf of NBCUniversal Media, LLC and its affiliates ('**Company**' or '**NBCUniversal'**). This Policy applies to all electronic media, data, or information that is (i) accessed, created, or shared using Company Systems, or via Company-paid access methods; or (ii) accessed, created, or shared for Company business purposes, even if on a personal device, such as the use of a personal phone to receive and send business emails.

NBCUniversal's computers, networks, communications systems, and other IT resources are intended for business purposes only (except for limited personal use as described below) during working time and at all other times. To protect NBCUniversal, its affiliates and its employees, it is the Company's policy to restrict the use of all IT resources and communications systems as described below. Each user is responsible for using these resources and systems in a productive, ethical, and lawful manner.

NBCUniversal's policies prohibiting harassment, namely the Respect in the Workplace Policy, apply to the use of the Company's IT resources and communications systems. No one may use any communications or computer system in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs, or any other characteristic protected by federal, state, or local law.

The use of Company Systems by employees signifies their understanding of and agreement to the terms and conditions of this Policy, as a condition of employment.

Certain jurisdictions and business units may impose more restrictive standards than those set forth in this Policy. In those circumstances, the more restrictive standards always apply. Employees must be familiar with the standards applicable to their jurisdiction and business unit.

2. Scope

This Policy covers any person who accesses NBCUniversal systems (each a '**System User**').

This Policy governs all IT resources, communications systems, applications, and data owned by or available at Company ('**Company Systems**'), and all use of such resources and systems when accessed using an employee's own resources, including but not limited to:

- Email systems and accounts
- Internet and intranet access
- Streaming devices
- Telephones and voicemail systems, including wired and mobile phones, smartphones
- Printers, photocopiers, and scanners
- All other associated computer, network, and communications systems, hardware, peripherals, and software, including network key fobs and other devices
- Closed-circuit television (CCTV) and all other physical security systems and devices, including access key cards and fobs

3. Requirements and Responsibilities

Company Systems are provided to conduct the Company's business for the Company's benefit. You must use Company Systems primarily for business purposes. Limited, reasonable use for personal purposes is permitted. You are responsible for the content of everything that you create, retrieve, or send using Company Systems.

a. **Monitoring of, and access to, Company Systems.** To the extent permitted by law, Company reserves the right to monitor the use of Company Systems using automated software or otherwise, and access/disclose information held within those systems. This is necessary for legitimate business reasons and to protect the Company's lawful interests, including for the following purposes: **information security management** (e.g. antivirus measures, data loss prevention), **business operations** (including access to Company mailboxes or files for business continuity purposes), **compliance with legal, regulatory, and policy requirements**, **litigation and investigations**, **subject access requests** (under applicable data privacy laws), and monitoring of **travel and expense records**. Any such monitoring by Company will be carried out in compliance with local laws and this Policy, and will be proportionate to the purpose of the monitoring.

Examples of information that may be monitored and accessed:

- Emails, messages, and other communications sent, received, stored, and archived on Company Systems, through email facilities or the Company network. This may include emails sent through private web-based email accounts on the corporate network
- Internet access including websites visited, archived content, and social network activities that are initiated from Company networks or devices. This may include the duration of site visits, search terms used in any search engine and attempts to access blocked sites
- All information stored or processed on Company devices
- Information stored in Company shared drives, home drives, cloud storage, etc.

Company reserves the right to remove any programs, applications, tools, data or other information or communications posted to, transmitted over, or accessed on Company Systems.

b. **Communications on Company Systems should not be considered private.** The monitoring and access described above applies to all information within Company Systems, including any personal use of Company Systems (see section 6 below). In order to protect your personal privacy, you should limit your use of Company Systems for personal purposes (e.g., do not use Company email for correspondence with your doctor or lawyer, do not use Company file storage to store personal medical, legal or financial documents, or personal photos). We strongly recommend that you mark personal emails as "private" or "personal" in the subject header.

c. **Certain access and actions may be blocked by the Company.** In order to protect Company Systems and ensure their efficient functioning, the Company reserves the right to block access to attachments to emails, restrict the sending of email messages by certain System Users, and block access to potentially objectionable or dangerous websites, tools, applications, platforms, or software.

d. **Use authorized Company Systems and software to conduct Company business.** You should only use Company-issued devices, software programs, cloud-based storage, or collaboration platforms to conduct Company business, unless you have been granted an exception. All devices and systems must be procured through authorized Company procurement processes, e.g., by submitting a request through ServiceNow. Collaboration tools approved for enterprise use are located here. The use of any additional tools should be approved by your manager or your business unit, in consultation with Cybersecurity, Information Technology, Legal and other stakeholders as appropriate. Regardless of which collaboration tools are used, you must comply with any document retention obligations specified in the Records and Information Management Policy. For additional guidance or system specific questions, please contact your Divisional IT Leadership or General Counsel.

e. **Bring Your Own Device.** In certain, limited circumstances, the Company may allow users limited access to its network through personally-owned devices, such as smartphones, tablets, other types of mobile computing devices and in personal computers. Such access is for business purposes only.

Permission to use a personal mobile device for business purposes is entirely at the discretion of the Company. The Company reserves the right to revoke this privilege at any time. Users must agree to all terms and conditions in NBCUniversal's Agreement for Use of Personally-Owned Mobile Devices prior to enrolment.

f. **Practice good 'housekeeping.'** You are encouraged to practice good 'computing housekeeping' – regularly clear unwanted items from email and and/or network folders and periodically delete them, unless subject to continued business need to retain and/or subject to a legal hold or instruction from Legal not to clear or delete items.

g. **Do not use personal email or messaging services for Company business** without preapproval from your Business Unit or region in consultation with Legal. This includes setting up your personal email on the default mail application of the Company-provided mobile device or registering your personal email at the account on a Company-

provided device (i.e., using your personal Apple ID). If you use a personal email account or messaging service for Company business, you must provide the Company, upon request, with the ability to access, collect and review communications concerning the Company's business, including account login information and written consent for a third-party service provider – for example Gmail or WhatsApp – to disclose to the Company all communications concerning the Company's business.

h. **You are the only person authorized to use the equipment and software issued to you.** You are not permitted to access a co-worker's computer, either physically or remotely via the network, without their express consent, or unless your role requires it (e.g., technician installing new software). NBCUniversal-provided or business-related username/password combinations must never be shared, written down or otherwise left in plain sight.

i. **Use authorized and encrypted removable media.** You must not store Company Confidential or Company Restricted data on unencrypted removable media, such as thumb drives, flash drives, zip drives, DVDs, CDs, and external hard drives. Approved encrypted media can be ordered through the TechLine. For more information on data classifications, review the Cyber Security Standard - Data Management.

j. **Duty to turn over Company-provided devices.** Employees must return all Company provided devices when they leave or when they receive an upgrade to a new device. If requested by the Company for the purposes mentioned in section 5(a) above, you must turn over any Company devices issued to you or in your possession, and allow the Company to access it, including by providing login information and any other assistance that the Company requires.

k. **You must return all Company-provided devices to the Company when you leave the Company.** If you are subject to a legal hold or instruction from Legal not to clear or delete items, you must not wipe any Company-provided device or delete any communications concerning Company business before you return it. You may be given further instructions in the offboarding process about assisting the Company with preserving and collecting information on your devices.

4. Personal Use of Company Systems

While Company Systems should be considered work tools, limited non-business use is permitted as long as it is not an abuse of Company time or resources, and is not contrary to other Company policies. Such personal use is a privilege and not a right. It must not be overused or abused. The Company may withdraw permission at any time or restrict access at its discretion. Personal use must meet the following conditions:

a. Use must not be for personal gain or profit
b. Use must not interfere with the performance of your duties
c. Use must not be in a manner that is unprofessional or unethical
d. Use must not place obligations on the Company or compromise its good name in any way, or interfere with the security controls the Company has deployed on its systems

e. Use must comply with NBCUniversal policies, including the Social Media Policy

If you are unsure about what constitutes acceptable use, you should consult your manager. Do not use Company Systems to conduct personal business ventures or other actions inconsistent with this Policy or in violation of NBCUniversal's Conflicts of Interest Policy or the Comcast Code of Conduct. Examples of such activity include using your Company email address for personal business purposes, or sending or posting advertisements or marketing mail.

5. Prohibited Uses

You must never use Company Systems for any inappropriate or unlawful conduct, including:

- Misrepresenting yourself as another individual or Company, including unauthorized use of another employee's account
- Sending, posting, recording, or encouraging conduct that violate our Respect in the Workplace Policy
- Revealing Company's proprietary or confidential information, or intellectual property without authorization
- Conducting or soliciting illegal activities
- Representing your personal opinion as that of Company's
- Interfering with the performance of your job or the jobs of other Company employees
- Unlawful, malicious, or unauthorized use of Company Systems, including attempting to circumvent any security or policy enforcement mechanisms, tampering with or disabling antivirus software, or otherwise compromising the security of Company Systems
- Storing or transmitting Company information on personally-owned devices or on unapproved collaboration tools, including removable media/portable storage media devices
- Any other use that violates Company's policies or the Code of Conduct

6. High Cyber Risk Travel Requirements

NBCUniversal Cyber Security restricts the use of NBCUniversal devices in regions or countries deemed to have a high cyber risk. Cyber Security maintains a listing of the high cyber risk countries and the specific required actions when travelling or becoming an expatriate to one of the countries. For a listing of those countries, along with the complete listing of guidance/actions required, click here.

If you are a permanent resident or an expatriate in one of the high cyber risk countries, you are not required to take any action while in your home country. However, if you travel to a different high cyber risk country, you must follow the required actions.

7. Incident Response

All System Users are responsible for reporting information security incidents, actual or suspected, by contacting the Cyber Security team at cyber@nbcuni.com.

8. Consequences of Violations

Failure to comply with this Policy may result in (i) removal of access to Company Systems; and/or (ii) disciplinary action, up to and including termination.

9. Related Resources

- NBCUniversal Agreement for Use of Personally-Owned Mobile Devices
- NBCUniversal Conflicts of Interest Policy
- NBCUniversal Cyber Security Data Management Standard
- NBCUniversal Information Security Policy
- NBCUniversal Social Media Policy
- NBCUniversal Records and Information Management Policy
- NBCUniversal Respect in the Workplace Policy

NBCUniversal

NBCUniversal
Operations & Technology
Cyber Security

NBCUniversal
Information Security Policy

Version 6.3

Effective: February 9, 2023

Table of Contents

1 Introduction

1.1 Scope

This *Information Security Policy* document applies to NBCUniversal Media, LLC (NBCUniversal), all business units, and subsidiaries globally.

1.2 Audience

This policy is intended for NBCUniversal and subsidiary employees, authorized agents, contractors, temporary workers, suppliers, and anyone charged with handling and accessing NBCUniversal information assets.

1.3 Key Terms

Subsidiary: All interest owned or controlled by NBCUniversal.

Systems: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

2 Document Structure

This policy contains various sections outlining information security objectives to be implemented by in-scope entities and draws from the ISO 27002:2015 and NIST standards.
The order of the sections, lists, and controls in this document do not imply their relative importance unless specifically stated. All items included in the policy should be held and observed with equal significance and enforced accordingly.
This document is meant to outline the framework of information security at NBCUniversal. Inclusion or exclusion from the policy should not be construed to imply acceptance or rejection of any particular topic. Contact your Business Area Information Security Officer (BA ISO) with any questions you have about this policy and related documents.

3 Risk Assessment and Treatment

NBCUniversal Cyber Security Organization assesses known and submitted risks to ensure that practical treatments are applied where necessary.
The NBCUniversal Governance Risk and Compliance (GRC) function is primarily responsible for generating the most current risk assessment documents, processes and forms.
The Security Architecture and Engineering (SA&E) team must be engaged to review all cyber, infrastructure and network related projects. For more information contact your BA ISO or cyber@nbcuni.com.

4 Information Security Policy

This policy sets forth management direction and support for information security at NBCUniversal and outlines operational and management responsibility to safeguard the Company from information security risks. The Company has issued this *Information Security Policy* to outline the measures and controls that every NBCUniversal business must have in place. This policy represents the minimum set of requirements that must exist for each business, unless a written exception is approved in accordance with Section 13.2 Exceptions.

4.1 Policy Management and Maintenance

This Information Security Policy can be found on the NBCUNow.
The Cyber Security Organization under the leadership of the Chief Information Security Officer of NBCUniversal maintains this *Information Security Policy* and supporting documents.

4.2 Business Addendums

If desired, each business may additionally create a business-specific information security policy that is more stringent than the requirements outlined in this policy. Business documents must reference this policy and itemize any additions or changes. Addendums must be reviewed and approved by the NBCUniversal Cyber Security Organization.

5 Organization of Information Security

5.1 Cyber Security Organization

NBCUniversal has created the Cyber Security Organization that is responsible for evaluation, communication, and enforcement of the information security requirements contained herein. Cyber Security roles and responsibilities are defined by the Chief Information Security Officer. They are reviewed and updated as necessary.

5.2 Business / Unit Information Security

Each business unit shall have a dedicated presence in information security that will serve as the Information Security leader for that business. This individual will be responsible for representing their business unit at all relevant meetings within the NBCUniversal Cyber Security Organization and report on specific security initiatives and issues within that business. This role shall be the Business Area Information Security Officer (BA ISO) or his/her designated representative.

5.3 Information Security Contacts

The current organization chart for the Cyber Security Organization for NBCUniversal and all affiliated business units is available by contacting cyber@nbcuni.com.

6 Asset Management

Proper management of computing assets is a key component of Information Security. Maintaining and proactively ensuring the security of these assets is an essential part of any operations team's responsibilities and must be treated as such. Assets include both physical (PCs, servers, IT infrastructure equipment, etc.) and logical assets (databases, applications, operating systems, software, etc.).

6.1 Systems and Application Registration

All systems (physical or logical) and applications, including websites, must be registered and maintained in a NBCUniversal asset management system (e.g., CMDB, CI/CD pipeline). Information on registration can be found by contacting NBC UNI ET Asset Configuration Management ETACM@NBCUni.com.

6.2 Information Classification and Data Management

All applications must be classified and controlled in accordance with the highest level of data maintained, processed, managed, or stored by the application. Individual components supporting an application may be subject to different controls depending on their function and the data they process, as directed by the information security leader, BA ISO or authorized representative.

Information on data management controls and the current data classification model can be found at the NBCUniversal Cyber Policy page.

7 Human Resource Security

7.1 Disciplinary Action for Non-Compliance / Violations

Violation of the NBCUniversal *Information Security Policy* or applicable Technology Security Standards may result in disciplinary action up to and including termination of employment or contract. This decision will be made in conjunction with the individual's manager and HR.

7.2 Training and Education

Personnel will be provided with appropriate information security training upon hire and periodically thereafter.

7.3 Termination or Change of Employment

Access rights must be promptly disabled for terminated or transferred personnel and reviewed at a minimum annually to identify users who require a change in access or no longer require access. Review processes must be documented. For more information, contact IRMO compliance or your BA ISO.

7.4 Recovery of Assets through Exit Process

Human Resources exit processes must include an IT asset recovery step to ensure all IT assets are returned upon termination.

7.5 Physical and Environmental Security Access Controls

Access to datacenters, server rooms, IT equipment rooms or other similar facilities must be controlled to prevent unauthorized access to NBCUniversal systems. For more information contact your BA ISO.

8 Communications and Operations Security

All NBCUniversal infrastructure and applications must comply with requirements specified in the relevant NBCUniversal Cyber Security Standards. All security standards are available on the Cyber Security website.

8.1 Operational Procedures and Responsibilities

Technology teams are responsible for development and maintenance of standard build documents that include required information security controls. For more information contact your BA ISO. All third-party engagements must comply with the security requirement defined in the *Third Party Security Standard.*

8.2 Back-up

Back-up data must be managed in a manner similar to production data with related information security controls in place and based upon data classification as defined in the *NBCUniversal Cyber Security Data Management Standard.*

8.3 Network Security Management

All networks must be designed or redesigned in accordance with security standards and with the engagement of the Security Architecture and Engineering team.

Third Party connections to the network must be reviewed by Security Architecture and Engineering; approved by the Chief Information Security Officer; documented, approved through a formal process; and ultimately comply with the *NBCUniversal Cyber Security IT Networks Security Standard.*

To engage cyber security, contact your BA ISO or send an email to cyber@nbcuni.com for more information.

8.4 Disposal and Re-Use of Technology Equipment

All technology equipment must follow a secure wiping process of at least one pass to purge all data and software prior to disposal or re-use. Refer to the *NBCUniversal Cyber Security Data Management Standard* for the detailed requirements.

8.5 Exchange of Information

Any system used to process, store or transfer NBCUniversal data must comply with controls as defined by the *NBCUniversal Cyber Security Data Management Standard*.

8.6 Security in Change Management

All business units must adhere to a change management process with representation from the cyber security team. For more information contact your BA ISO.

8.7 Asset Acquisition

Acquisition of technology assets must follow an approved Sourcing process. Refer to the *NBCUniversal Cyber Security Device Management Standard.*

8.8 New Technology Introduction

Introduction of new technologies (hardware, software, systems) into the NBCUniversal environment must be approved by NBCUniversal Information Technology.

9 Access Control

9.1 Business Requirement for Access Control

Roles for user access must be defined for all applications and environments. Access controls must be implemented to limit access to networks, databases, operating systems, VPN, Security Tokens, and applications to authorized individuals based upon access roles.

Separation of duties for critical functions shall be sufficient to ensure no individual has the ability to enable fraud, compromise, abuse or errors without detection. This includes separating key functions including but not limited to: Access authorization and IT administration; IT Management and IT Administration; Security Monitoring and Response and IT Administration.

To prevent misuse of the system, user's access should be commensurate with their duties and based on the principle of least privilege. Only the minimum necessary rights should be assigned to a subject that requests access to a resource where technically feasible.

9.2 Identification and Authentication

User access must be authenticated and authorized prior to granting access to controlled computing resources. Authentication management systems must comply with the controls as outlined in the *NBCUniversal Cyber Security Identification and Authentication Standard.*

9.3 User Access Management

Identity lifecycle management (registration, authorization, and revocation) processes must be documented and enforced.
Refer to the *NBCUniversal Cyber Security Identification and Authentication Standard* for additional information.

9.4 Privilege Management

Highly privileged accounts must be identified, documented, restricted, and controlled as defined in the *NBCUniversal Cyber Security Identification and Authentication Standard.*

9.5 Network Access Control

Access to company networks must be restricted to approved devices and users and comply with controls in accordance with the *NBCUniversal Cyber Security IT Networks Security Standard*.

9.6 Mobile Computing and Remote Working

Remote connections to the network must comply with controls outlined in the *NBCUniversal Cyber Security IT Networks Security Standard* and *NBCUniversal Cyber Security Device Management Standard*.

10 System Acquisition, Development and Maintenance

Security requirements for information systems can be found in related Cyber Security Standard documents located at the NBCUniversal Cyber Policy page.

10.1 Cryptographic Encryption Controls

The Chief Information Security Officer will approve and enforce encryption tools, encryption, and key management. Businesses must adhere to cryptographic controls as dictated by Security Engineering and Architecture.

10.2 Security of System Files

Individuals must not install disallowed software and all software must comply with the *NBCUniversal Acceptable Use Policy* and related security standards. Individuals must not modify, disable, or otherwise alter any Information Security hardware or software.

10.3 Security in Development and Support Processes

Application development must adhere to the *NBCUniversal Cyber Security Secure Software Development Standard* and to the guidance defined in the Information Security Guideline for Secure Coding.
IT and application support processes must comply with all aspects of this policy and related requirements defined in Cyber Security Standards located on the Cyber Policy page.

10.4 Third-Party Application and Business Process Management

When third parties are employed to develop and maintain applications, these third parties must undergo a supplier security review and comply with additional controls as defined by the *Third Party Security Standard*. In addition, the requirements outlined in the *NBCUniversal Cyber Security Secure Software Development Standard* must be implemented and managed. For more information about the supplier security review process, please email: supplier.security@nbcuni.com and see Section 14 Supplier Relationships.

10.5 Protection of Non-Production Data

Non-production environments must not use sensitive business, personnel, or customer data, such as unmasked personal information or intellectual property. Where this is not possible, controls must be applied in accordance with the highest level of data classification. For more information on the use of data in non-production environments, please contact cyber@nbcuni.com.

10.6 Technical Vulnerability Management

NBCUniversal Cyber Security must address vulnerabilities in the environment and is responsible for evaluating new risks, defining patching requirements, approving mitigation plans, and testing for vulnerabilities.
Individuals must not attempt to identify, test, or validate potential vulnerabilities in applications or within the NBCUniversal IT infrastructure. Individuals must report suspected or encountered IT vulnerabilities to their BA ISO or by sending an email to cyber@nbcuni.com.

11 Information Security Incident Management

11.1 Reporting Information Security Events and Weaknesses

Individuals must report information security concerns and incidents by sending an email to cyber@nbcuni.com or calling the Cyber Security Response Operations Center (ROC) at 1855-650- SAFE (7233).

11.2 Management of Information Security Incidents and Improvements

Incidents must be managed in accordance with the *NBCUniversal Cyber Security Incident Response* playbook under the direction of the Chief Information Security Officer.

12 Business Continuity Management

Business continuity and disaster recovery process and operations must meet the requirements of this policy and the related security standards.
Applications, infrastructure systems and technology services must comply with the *Business Continuity and Crisis Management* policy.

13 Compliance

13.1 Legal Requirements

Requirements in this policy and supporting documents are designed to meet or exceed regulatory, legal, or contractual obligation. If anyone believes that these requirements conflict with local law, then contact the Chief Information Security Officer by sending an email to cyber@nbcuni.com.com.

13.2 Exceptions

Exceptions to this policy must be submitted through the Policy Exception Request (PER) process as defined on the NBCUniversal Cyber Security website and approved in accordance with the policy exception management process.

13.3 Information Systems Audit

Testing and audits related to information security must be coordinated through the Cyber Security Organization.

13.4 Measurements and Reporting

Metrics related to the information security programs and protections will be collected and analyzed by the Cyber Security Organization.

14 Supplier Relationships

14.1 Addressing Security within Supplier Agreements

NBCUniversal must establish minimum security requirements as part of any contractual agreement with a supplier where the supplier will handle NBCUniversal Data and/or have access to NBCUniversal Systems. (Terms are defined in the *Third Party Security Standard*.)

The *Third Party Security Standard* provides the baseline security requirements for suppliers and any other third parties who manage or access to NBCUniversal Data or have a connection to the NBCUniversal network. Exceptions to the baseline security requirements must be reviewed and approved by the Cyber Security Organization.

14.2 Supplier Service Delivery Management

Any entity, organization, or individual that has access to NBCUniversal Data, NBCUniversal Systems, or property, to provide services to NBCUniversal (including hosting or development services) must go through the supplier review process.

To initiate the supplier security review process, please contact your BA ISO or supplier.security@nbcuni.com.

Document Information

Document Name	Information Security Policy
Version	6.3
Last Reviewed	February 9, 2023

Revision History

Version	Date Released	Changes	Author	Approved

3	April 15, 2015	Annual Review; Updated Links to Information Security Website	NBCUniversal Cyber Security	NBCUniversal CISO
4	August 2016	Updated links, documents, points of contact and references.	NBCUniversal Cyber Security	NBCUniversal CISO
5	May 2017	Aligned with latest version of ISO27002, outside Counsel review, updated titles, terms and terminologies. Re- reviewed by new Sr. Counsel, W. Chua.	NBCUniversal Cyber Security	NBCUniversal CISO
6	November 2018	Redline to align with transformation.	NBCUniversal Cyber Security	NBCUniversal CISO
6.1	February 2019	Reviewed and updated section 9 to refer to Identification and Authentication. Corrected section 10.4 to refer to section 14 not 15.	NBCUniversal Cyber Security	NBCUniversal CISO
6.1	December 19, 2020	Reviewed without changes	NBCUniversal Cyber Security	NBCUniversal CISO
6.2	August 30, 2022	• Updated 1.1 Scope and 1.2 Audience to add subsidiaries for clarity. Also in Section 1.1 Scope, completed NBCU's name so it now reads: NBCUniversal Media, LLC (NBCUniversal). • Added section 1.3 Key Terms and defined subsidiary (as given by Legal) and systems. • Added to Section 5.1: "Cyber Security roles and responsibilities are defined by the Chief Information Security Officer. They are reviewed and updated as necessary." • In Section 5.2, deleted the clause: "with dotted line reporting to the NBCUniversal Chief Information Security Officer." • In Section 6.0 Asset Management, deleted the second paragraph, which was repeated in Section 6.1. • In Section 6.1:	NBCUniversal Cyber Security	NBCUniversal CISO

Version	Date Released	Changes	Author	Approved

		○ Changed the header to: "Systems and Application registration" ○ Added "systems (physical or logical) and" in the first sentence ○ Deleted "application" before asset management system ○ Added parenthetical (e.g., CMDB, CI/CD pipeline) after "asset management system" Replaced "contacting your BA ISO" with "contacting NBC UNI ET Asset Configuration Management ETACM@NBCUni.com." • Section 9.0 Access Control. Added two paragraphs to section 9.1: ○ "Separation of duties for critical functions shall be sufficient to ensure no individual has the ability to enable fraud, compromise, abuse or errors without detection. This includes separating key functions including but not limited to: Access authorization and IT administration; IT Management and IT Administration; Security Monitoring and Response and IT Administration. ○ To prevent misuse of the system, user's access should be commensurate with their duties and based on the principle of least privilege. Only the minimum necessary rights should be assigned to a subject that requests access to a resource where technically feasible." ○ Changed the reference in Section 12 to read: *Business Continuity and Crisis Management* policy.		
6.3	February 9, 2023	• Updated Section 10.3 to reflect the actual name of the standard: *NBCUniversal Cyber Security Secure Software Development Standard.* • Adjusted the sentence in Section 6.1 from "the" to "a" "NBCUniversal asset management system…" to	Cyber Security – GRC Governance	NBCUniversal CISO

Version	Date Released	Changes	Author	Approved

		clarify there is no one central CMDB CI/CD pipeline but several. • Adjusted font and sub-head capitalization for consistency. • Adjusted the titles of referenced documents to match the current titles. • Replaced “personally identifiable information” with the updated term “personal information.” • Replaced the logo on the title page with an updated one.		