

## GLOBAL PRIVACY RIDER

This Global Privacy Rider governs the Processing of Personal Information pursuant to the agreement between SIE and Vendor (each a **“party”** and together the **“parties”**), including any SOWs (the **“Agreement”**). The terms of this Global Privacy Rider include those in any Schedules, Annexes, Cross-Border Transfer Agreements, or other data processing terms between the parties that may be incorporated by reference (collectively the **“Privacy Rider”** unless otherwise indicated). This Privacy Rider forms an integral part of the Agreement between the parties. In the event of any conflict between the provisions of this Privacy Rider and other provisions in the Agreement, this Privacy Rider shall prevail and shall apply instead of those other provisions of the Agreement regardless of anything in the Agreement purporting to resolve the conflict.

### **1. Definitions.** For purposes of this Privacy Rider:

- 1.1. “Applicable Data Protection Law”** means any privacy or data protection laws or regulations in any jurisdiction applicable to the Processing of SIE Personal Information by Vendor pursuant to the Agreement (e.g., the United Kingdom Data Protection Act of 2018 and any other national laws arising by virtue of Section 3 of the European Union (Withdrawal) Act of 2018; European laws (e.g., the General Data Protection Regulation (EU) 2016/679); US federal and state laws (e.g. the California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq.); the Japan Act on the Protection of Personal Information (Act No. 57 of 2003); the Republic of Korea Personal Information Protection Act 2011; the Brazil General Data Protection Law nº 13709/2018; electronics communications laws), and including as such laws or regulations may be replaced, amended, or superseded from time to time.
- 1.2. “Personal Information”** means (a) any information that, alone or in combination, directly or indirectly, relates to, or is capable of being associated with, or could reasonably be linked to, or describes, an identified or identifiable natural person or group of persons, including, for example, direct identifiers such as name or email address, or indirect identifiers such as IP address or account ID, or a combination of data that enables identification, and (b) any information as defined by similar terms under Applicable Data Protection Law.
- 1.3. “Process”, “Processed”, or “Processing”** means any operation or set of operations performed on any and all data or information through Vendor’s performance of the Agreement, including its creation, collection, use, storage, retention, disclosure, and destruction.
- 1.4. “SIE”** means the Sony Interactive company that entered into the Agreement, and other Sony Interactive Entertainment group company, affiliate, or subsidiary on behalf of which the Agreement is signed.
- 1.5. “Sell” or “Sale”** means renting, releasing, disclosing, disseminating, or otherwise making available Personal Information to any other party for monetary or other valuable consideration.
- 1.6. “Sensitive Personal Information”** means (a) Personal Information revealing or concerning a known child, racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, criminal conviction or offense information, genetic data, biometric data, precise geolocation, electronic communications including voice data and message content, video or media streaming history, safety and moderation data, medical or health information, sex life or sexual orientation, citizenship or immigration status, government-issued identification, account credentials, and financial account or payment card information, and (b) any information defined by similar terms as sensitive under Applicable Data Protection Law.
- 1.7. “Share”** means sharing, renting, releasing, disclosing, disseminating, or otherwise making available Personal Information to a third party for cross-contextual behavioral advertising as defined under the California Privacy Rights Act.
- 1.8. “SIE Personal Information”** means any and all Personal Information in any form that is (a) disclosed or furnished by SIE to Vendor or (b) otherwise Processed by Vendor in the context of the Agreement or this Privacy Rider.
- 1.9. “SOW”** means any statement of work entered into between the parties pursuant to the Agreement.
- 1.10. “Vendor”** means the entity that entered into the Agreement with SIE that is Processing SIE Personal Information on behalf of SIE.

### **2. Processing of SIE Personal Information**

- 2.1. SIE hereby instructs Vendor and Vendor agrees to Process SIE Personal Information solely in accordance with Applicable Data Protection Laws and SIE's documented instructions, including as set forth in the Agreement. Vendor shall not Sell, Share, or otherwise Process SIE Personal Information outside of the direct business relationship between Vendor and SIE. Vendor shall not Process SIE Personal Information, including in anonymous or aggregate form, for Vendor's own purposes or benefit, including for analysis, building or improving the quality of Vendor's products or services, or other commercial uses. If Vendor is required by law to Process SIE Personal Information for any other purpose, Vendor shall provide SIE with advance written notice of the Processing and the specific legal requirement unless the law expressly prohibits such notice. Upon receiving such notice, SIE may, in its discretion, immediately suspend all Processing of SIE Personal Information by Vendor or terminate the Agreement.
- 2.2. Vendor will ensure that any access to SIE Personal Information by its employees, contractors, personnel, or other agents is strictly limited to only those who need to know, have committed themselves to confidentiality, and have received appropriate training on relevant aspects of Applicable Data Protection Law.
3. **Subprocessors.** Vendor shall not allow or engage any other party to Process SIE Personal Information (a "**Subprocessor**") unless the Subprocessor has been authorized by SIE pursuant to the terms of this Section and is bound by a written agreement with Vendor that includes data protection obligations no less protective than those contained in this Privacy Rider and that are consistent with Applicable Data Protection Law. SIE consents to the engagement of the Vendor's Subprocessors listed in the Agreement. Vendor will notify SIE of any additional or replacement Subprocessors at SIE-Vendor-Notifications@sony.com. Any failure by SIE to object to such notice within thirty (30) days of receipt shall be deemed SIE's authorization to engage such Subprocessor. Vendor remains fully responsible and liable to SIE for any failure by a Subprocessor to fulfil its obligations under Applicable Data Protection Law and this Privacy Rider. Vendor shall notify SIE of any failure by any Subprocessor to fulfil its obligations under Applicable Data Protection Law. SIE may at any time revoke authorization if it has reasonable grounds to doubt a Subprocessor's ability comply with Applicable Data Protection Law.
4. **Security.** Vendor shall maintain reasonable and appropriate technical and organizational measures to ensure the security, confidentiality, and integrity of SIE Personal Information. The minimum technical and organizational measures to be implemented by Vendor are set forth in Schedule 1 to this Privacy Rider. In the event SIE Personal Information is involved in an Information Security Incident, as defined in Schedule 1, Vendor shall meet all its obligations set out in Schedule 1 and Applicable Data Protection Law.
5. **Cooperation and Audits**
- 5.1. Vendor shall, to the extent legally permitted, notify SIE at siee.dpo@sony.com within three (3) days if Vendor receives an audit request, complaint, or other inquiry from a supervisory authority, regulator, or other third party that relates to the Processing of SIE Personal Information (a "**Request**"). Vendor shall assist SIE in responding to such Request, including by providing access to, copies of, or deleting SIE Personal Information or producing records, reports, summaries, or other information.
- 5.2. Vendor will cooperate with and reasonably assist SIE to ensure the parties meet their obligations under Applicable Data Protection Law, including in relation to information security, data protection impact assessments, cross-border transfer risk assessments, or consultation with supervisory authorities.
- 5.3. At SIE's request, Vendor shall make available to SIE all information reasonably necessary to demonstrate compliance with Vendor's obligations under this Privacy Rider and to allow for audits conducted by SIE or an independent third-party auditor mutually agreed to by the parties. If at any time, Vendor is unable to comply with Vendor's obligations, Vendor shall notify SIE in writing. SIE may, in its discretion, immediately suspend any Processing of SIE Personal Information or terminate the Agreement if Vendor is unable to sufficiently demonstrate compliance.
6. **Cross-Border Transfers.** Where SIE Personal Information is subject to Applicable Data Protection Law that restricts the export, transfer, or onward transfer of such Personal Information to a certain country (a "**Restricted Transfer**"), the following terms apply.

- 6.1. Where a Restricted Transfer concerns Personal Information that relates to individuals located in or that is otherwise subject to Applicable Data Protection Laws of the United Kingdom, Europe, or Switzerland, Sony Interactive Entertainment Europe Limited (10 Great Marlborough Street, London, W1F 7LP, United Kingdom; tel.: +44 (0)20 7859 5000; e-mail: [siee.dpo@sony.com](mailto:siee.dpo@sony.com); company no. 03277793) (“SIEE”) is accountable as the controller. Such Restricted Transfers may only occur pursuant to an adequacy decision or appropriate safeguards, including an approved code of conduct, certification mechanism, or standard data protection clauses. To the extent applicable, the parties hereby agree to enter into and be bound by the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 and approved by the European Commission decision 2021/914, dated 4 June 2021 (“EU SCCs”) and the International Data Transfer Addendum to the EU SCCs version B1.0, issued by the UK Information Commissioner’s Office and laid before the Parliament in accordance with s119A of the Data Protection Act 2018, in force 21 March 2022 (“UK Addendum”), including as may be replaced, amended, or superseded, and the current versions of which are available at <https://www.playstation.com/en-gb/sie-eusccs-ukidta/>. The EU SCCs and UK Addendum are incorporated herein by reference as follows:
- 6.1.1. With respect to Restricted Transfers between SIEE and Vendor, Module 2 for Controller-to-Processor Transfers applies and SIEE is the “controller” and “data exporter” and Vendor is the “processor” and “data importer”.
- 6.1.2. With respect to any Restricted Transfers between Sony Interactive Entertainment, LLC, Sony Interactive Entertainment, Inc., or any other SIE Group Company acting as a processor that is a signatory to the Agreement, Module 3 for Processor-to-Processor Transfers applies and SIEE is the “controller”, the other SIE Group Company is a “processor” and “data exporter”, and Vendor is the other “processor” and “data importer”.
- 6.2. Where a Restricted Transfer concerns SIE Personal Information that is subject to any other Applicable Data Protection Law, including Argentina, Brazil, Columbia, or Uruguay, the parties hereby enter into and agree to be bound by any other appropriate transfer mechanisms or country-specific agreements required to transfer SIE Personal Information (e.g., <http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm>) (collectively with the transfer mechanisms listed in this Section “**Cross-Border Transfer Agreements**”). In the event of any conflict between the provisions of this Privacy Rider and other provisions in any Cross-Border Transfer Agreements, the other provisions of the Cross-Border Transfer Agreements shall prevail and apply instead solely with respect to the regional or country-specific Processing addressed therein.
- 6.3. If requested by SIE, Vendor shall implement any further Cross-Border Transfer Agreements or take any other steps as may be reasonably required to ensure all Restricted Transfers are conducted in compliance with Applicable Data Protection Law. If Vendor fails to do so, SIE may, in its discretion, immediately suspend any Processing of SIE Personal Information or terminate the Agreement.

## 7. Miscellaneous

- 7.1. Vendor’s failure to comply with any of the obligations as set forth in this Privacy Rider shall be considered Vendor’s material breach of the Agreement.
- 7.2. In addition to any indemnification obligations elsewhere in the Agreement, Vendor agrees to indemnify, defend, and hold harmless SIE and its affiliates, subsidiaries, successors and assigns (and their officers, directors, employees, sublicensees, customers and agents) from and against any and all claims, losses, demands, liabilities, damages, settlements, expenses and costs (including attorneys’ fees and costs), arising from an Information Security Incident or Vendor’s failure to comply with any of its obligations in this Privacy Rider or Applicable Data Protection Law. This indemnification obligation is not subject to any limitation of liability elsewhere in the Agreement.
- 7.3. The provisions of this Privacy Rider will survive the expiration or earlier termination of the Agreement and will only cease once Vendor ceases to Process any and all SIE Personal Information.

## SCHEDULE 1

### TECHNICAL AND ORGANIZATIONAL MEASURES

1. **Definitions.** Any capitalized terms not otherwise defined herein have the same meanings set forth in the Privacy Rider.
  - 1.1. **"Data"** means any and all data and information, including confidential information, Personal Information, PCI-DSS Data, etc.). SIE Data is Confidential Information as that term is defined in the Agreement.
  - 1.2. **"Information Security Incident"** or **"Incident"** means the following: (a) Processing of SIE Data in violation of the Agreement including this Schedule 1; (b) a breach of confidentiality, integrity, or availability of SIE Systems, SIE Data, or Vendor Systems; or (c) breach of Applicable Data Protection Laws.
  - 1.3. **"PCI-DSS Data"** means data that is a credit or debit card holder's credit or debit card account number, bank account number, name, service code, security code, card validation code or value (e.g., CVV number), expiration date, magnetic stripe data, PIN, PIN block, or password or that is otherwise subject to the Payment Card Industry Data Security Standards.
  - 1.4. **"Services"** means any services that the Vendor provides under the Agreement.
  - 1.5. **"SIE"** in combination with the terms **"Data"** or **"PCI-DSS Data"** means the respective subsets of such data that are received or created by Vendor from or on behalf of SIE, its affiliates, subsidiaries, agents, or employees, in connection with Vendor's performance of the Services.
  - 1.6. **"SIE Systems"** means SIE's (including its affiliates and subsidiaries) information systems, mobile devices, applications, databases, infrastructure, platforms, products, and networks.
  - 1.7. **"Vendor Systems"** means Vendor's information systems, mobile devices, processes, facilities, applications, databases, infrastructure, platforms, products and networks that (a) are utilized to provide the Services, (b) Process SIE Data, and/or (c) access, connect to, use or otherwise interact with SIE Systems.
2. **Processing Solely for SIE; Solely by Vendor.** Vendor agrees that it will not Process SIE Data for any purpose other than as necessary and for as long as necessary for the specific purpose of performing the Services specified in the Agreement on behalf of SIE. For purposes of clarity, Vendor shall not Process any SIE Data if such Processing is no longer necessary to perform the Services. Vendor may not further delegate any performance of its Services to any other party without SIE's authorization and consistent with the procedures set out in Section 8 below.
3. **Information Security Program and Requirements.**
  - 3.1. Vendor will implement, maintain, and comply with a written information security program ("**Information Security Program**") to (a) ensure the security, availability, integrity or confidentiality of Vendor Systems and SIE Data, (b) identify and protect against potential threats or hazards to Vendor Systems and SIE Data, and (c) protect against unauthorized access to, use of, alteration of or destruction of Vendor Systems and SIE Data.
  - 3.2. Vendor will update the Information Security Program, as appropriate, in light of (a) any relevant changes in technology or industry security standards; (b) the sensitivity of SIE Data; (c) internal or external threats to Vendor Systems, SIE Systems, and SIE Data; (d) SIE's instructions pursuant to Section 3.1; (e) requirements of applicable work orders; and, (f) Vendor's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.
  - 3.3. Vendor will, at a minimum, include or address the following safeguards and requirements in its Information Security Program:
    - 3.3.1. **Information Security Assessment.** Vendor will: (a) implement an audit program, at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing SIE Data, to test for and, if necessary, remediate reasonably foreseeable or identified internal and external risks of any security controls; (b) conduct, in line with ISO27001 or similar standards, an annual risk assessment that assesses the threats and vulnerabilities associated with Vendor Systems, or Vendor's other processes, facilities, and system components Processing SIE Data; and, (c) produce (pursuant to the results of (a) and (b)) a documented risk assessment and, where appropriate, a risk remediation plan.
    - 3.3.2. **Assigned Security Responsibility.** Vendor will designate a security official employed at management level or above to be responsible for the development, implementation, and ongoing maintenance of its

Information Security Program. Such employee will have appropriate recognized Information Security credentials and qualifications. Vendor will promptly communicate its appointed security official to SIE to be SIE's primary point of contact to address questions or issues regarding Vendor Systems, Vendor's Incident Response Plan (as provided in Section 4 below) or an Information Security Incident.

**3.3.3. Secure Authentication Protocols and Access Control Measures.** Vendor will implement and maintain Secure Authentication Protocols and Access Control Measures (defined below) and other policies, procedures, and physical and technical controls designed to (a) limit access to or use of Vendor Systems, SIE Systems, and SIE Data and the facilities in which they are housed to a limited number of properly authorized persons, each of whom are under an obligation (written or by policy) of confidentiality and non-disclosure, having a need for such access or use to perform the Services, and authorized to access or use such Data and Systems solely as necessary to perform the Services; (b) ensure that all persons having logical or physical access to Vendor Systems, SIE Systems, and SIE Data have appropriately controlled and limited access and use, and to prevent others who should not have access (including, without limitation, terminated employees) from obtaining access or use; (c) prohibit persons from making copies or reproductions of SIE Data or otherwise transmitting SIE Data, except to the extent necessary solely to perform the Services, in which case all such copies, reproductions, and transmissions will be deemed SIE Data; and (d) to include multi-factor authentication for accounts which have remote access, access to or use of SIE Data, and administration access or privileged account permissions. These "**Secure Authentication Protocols and Access Control Measures**" include (a) use of secure user authentication protocols, including control of user IDs and other identifiers, as well as the assignment of unique identifications plus passwords (which are not Vendor-supplied default passwords) to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access control); (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies (such as biometrics or token devices); (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the information they protect (in particular, passwords must be encrypted or stored using a salted hash); (d) restricting access and use to active users and active user accounts only; (e) blocking access and use to user identification after multiple unsuccessful attempts to gain access or use or the limitation placed on access and use for the particular system; and (f) requiring management approval for administrative user access to or use of SIE Data or SIE Systems with such administrative user sessions expiring within five (5) minutes.

**3.3.4. ISO 27001 Certification.** Vendor shall maintain and continue to have certification to ISO 27001; and promptly provide SIE with copies of its ISO27001 certificate and statement of applicability.

**3.3.5. Device and Media Controls.** Vendor will ensure that all media containing SIE Data sent outside its facilities is logged, authorized by management, and sent via secured courier or other delivery method that can be tracked. Vendor will encrypt all back-up/archive media containing SIE Data and restrict access and use to all off-site backup/archive media to appropriate authorized personnel. Vendor shall ensure that no SIE Data is stored on any portable medium or device, including laptops, mobile devices, and removable media, except when strictly necessary for the performance of the Services and such portable media or devices containing SIE Data are encrypted.

**3.3.5.1. System, Storage and Transmission Security.** Unless otherwise approved in writing by SIE, Vendor will implement and maintain physical and technical controls to: (a) restrict access to or use or disruption or altering or copying or removal of the Vendor Systems and SIE Data (including when SIE Data is transmitted over an electronic communications network or while being recorded onto data carriers); (b) ensure that no SIE Data is physically co-mingled with any of Vendor's (or any third party's) other data, or virtually co-mingled with other data where such SIE Data shares the same media, device, or system, unless the data is logically separated; (c) implement firewall protection, router configuration rules and standards to maintain the integrity of SIE Data and that restrict connections between untrusted networks and any system components in the environment; (d) establish up-to-date application security firewalls to ensure protection of Layer 7 and other application platform oriented threats and regular testing of such firewalls to ensure the effectiveness of application oriented threat mitigation by application layer firewalls; and (e) implement no less than industry standard encryption technology that has been adopted by an

established standards setting body, including, but not limited to, the National Institute of Standards and Technology, with respect to all records and files containing SIE Data either at rest or in transit, including, all SIE Data to be transmitted across public networks or wirelessly, and all SIE Data stored on laptops, servers, or removable media. With respect to (e), above, Vendor's encryption algorithms shall meet the following criteria: (i) de facto cryptographic standard protocols (e.g., SSL, TLS, SSHv2, SFTP, IPSec, PGP, S/MIME, etc.); (ii) proven, standard algorithms as the basis for encryption technologies (e.g., AES, 3DES, RSA, etc.); and, (iii) the length of the cryptographic key will meet the following guidelines: (1) symmetric cryptosystem key lengths must be at least 128 bits or 3DES strength, and (2) asymmetric cryptosystem keys must be of a length equivalent to or more than the strength of 2048 bits for the RSA algorithm.

**3.3.5.2.** Vendor shall protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology and implement appropriate management and safeguards of cryptographic keys.

**3.3.6. System Testing and Maintenance.** Vendor shall test, detect, and prevent security system failures, maintain Vendor Systems, and ensure a level of security appropriate to the risk. Such measures include: (a) installing operating system and application Critical Security Patches that are reasonably designed to maintain the integrity of SIE Data within thirty (30) days of publication, and within three (3) months for other types of patches and updates; (b) installing the latest recommended versions of operating systems, software and firmware for all Vendor Systems components; and (c) ensuring up-to-date system security agent software, which includes malware protection and is set to receive automatically updated (at least daily) patches and virus definitions.

**3.3.7. Scanning and Testing; Vulnerability Remediation.** At least once per month, Vendor will perform internal system and application vulnerability assessments and external web (and other, if applicable) application and infrastructure vulnerability assessments on all Vendor Systems used to provide the Services. In addition to meeting the requirements of routine updates to systems defined in Section 3.3.6, Vendor will promptly correct any vulnerability or security issue discovered in Vendor Systems that may reasonably impact the confidentiality, integrity, or availability of SIE Data based on the Common Vulnerability Scoring System ("CVSS") v3.1 Temporal score of the vulnerability discovered as follows:

**3.3.7.1.** For external facing vulnerabilities:

**3.3.7.1.1.** A score of 9.0 or above: Vendor will remediate such vulnerability within one (1) business day;

**3.3.7.1.2.** A score between 7.0 and 8.9: Vendor will remediate such vulnerability within seven (7) business days;

**3.3.7.1.3.** A score between 4.0 and 6.9: Vendor will remediate such vulnerability within thirty (30) business days;

**3.3.7.1.4.** A score under 4.0: Vendor will remediate such vulnerability within a reasonable time.

**3.3.7.2.** For internal facing vulnerabilities:

**3.3.7.2.1.** A score of 7.0 or above: Vendor will remediate such vulnerability before the next production release, not to exceed thirty (30) days;

**3.3.7.2.2.** A score between 4.0 and 6.9: Vendor will remediate such vulnerability before the next production release, not to exceed one hundred and twenty (120) days;

**3.3.7.2.3.** A score under 4.0: Vendor will remediate such vulnerability within a reasonable time.

**3.3.8. Security Awareness and Training; Discipline.** Vendor will establish and maintain an ongoing security awareness and training program for all Vendor personnel (including management, employees, contractors and other agents with access to or use of SIE Data, Vendor Systems, or SIE Systems), which includes (a) training on the importance of information security and how to implement and comply with Vendor's Information Security Program, including the proper use of the Vendor's computer security systems and compliance with Vendor's security policies relating to the storage, access, use and transportation of

records containing SIE Data outside of business premises; and (b) disciplinary measures for violation of the Information Security Program.

**3.3.9. Contingency Planning.** Vendor's Information Security Program will also address any occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages or destroys Vendor Systems or SIE Data, including a data backup plan and a disaster recovery plan with, at least, annual testing of such plans and continuous improvement of such plans.

**3.3.10. Logging.** Vendor will record access logs (including without limitation timestamp, source IP address, resource path, and event descriptions) and examine activity in Vendor Systems that contain or use electronic information, including appropriate logs and reports concerning the security requirements set forth herein. Upon SIE request, Vendor will promptly provide such records and reports to SIE. Vendor will keep such logs for a period of at least twelve (12) months, except for logs related to SIE Data that would be categorized as within the scope of the Sarbanes-Oxley Act of 2002, where these logs shall be maintained for seven (7) years.

**3.3.11. Public Clouds.** Vendor shall obtain written consent from the SIE Security Official identified below prior to migrating any part of its Services from a hosted solution to a "public cloud" service provided, however, that no such notice shall be required if the service is owned by any of the following public cloud service providers: Amazon Web Service (AWS), Microsoft Azure, Google Cloud, Alibaba Cloud, IBM Cloud, or Salesforce.

**3.4.** Vendor will maintain appropriate and complete documentation describing the Information Security Program it maintains in accordance with the terms herein and will provide such documentation to SIE upon request.

#### **4. Notification of Information Security Incident; Incident Response Plan; Remedial Action.**

**4.1. Incident Response.** Immediately upon reasonable suspicion or confirmation that an Incident has occurred, Vendor will take all measures to ensure the parties' compliance with Applicable Data Protection laws, including:

**4.1.1.** Initiate all commercially reasonable efforts to determine the occurrence, cause, scope and severity of the Incident;

**4.1.2.** Initiate all commercially reasonable efforts to mitigate the Incident without detriment to the efforts to investigate the breach; and,

**4.1.3.** Fully assist SIE and any governmental authority of competent jurisdiction with investigating the Information Security Incident. In addition, if SIE's investigation of the Information Security Incident is not commercially practicable, Vendor will engage, at its sole cost, a mutually agreeable third party to conduct the investigation.

**4.2. Notification to SIE.** Vendor will notify SIE Information Security at:

**SIE Information Security Official**  
**Security Operations Center**  
**Phone (primary): +1 (858) 207-1691**  
**Phone (secondary): +1 (858) 207-1692**  
**Email: [SIE-CIDC@sony.com](mailto:SIE-CIDC@sony.com)**

**4.2.1.** Within one (1) hour, via telephone and email:

**4.2.1.1.** The name, phone number, and email address of Vendor's contact point related to the incident.

**4.2.1.2.** A summary of the facts and reasoning that give rise to Vendor's suspicion that an Incident has occurred.

**4.2.2.** Within twelve (12) hours, via email: A written report describing the SIE Data or SIE Systems affected, and the actions being taken by Vendor to determine and mitigate the extent and scope of the incident and prevent its recurrence.

**4.3. Remedial Action.** Upon resolution of the Incident, Vendor will take the following remedial actions:

**4.3.1.** Provide SIE with satisfactory assurance that such Information Security Incident or potential Information Security Incident will not recur, as well as a description of the resulting forensic and remediation efforts and outcomes of such efforts.

**4.3.2.** Notify SIE if, at any time, Vendor becomes aware of any third-party claims or legal process relating to the Incident;

- 4.3.3. Promptly correct any causes of the Incident and, unless such incident was solely caused by SIE, these corrections shall be at no additional charge to SIE;
- 4.3.4. Fully assist SIE and any regulator or other governmental body by providing oversight over the Information Security Incident in remedying and taking any other action SIE deems necessary regarding the Information Security Incident and any dispute, inquiry, or claim that concerns the Information Security Incident;
- 4.3.5. Undertake any other remedial measures SIE deems necessary including, notice, credit monitoring services, and the establishment of a call center to respond to inquiries.

4.4. **Additional Notifications.** At SIE's request Vendor will provide notification to public authorities, individuals, or any other persons and take any other remedial actions, at Vendor's sole cost and expense, which SIE deems necessary in its sole discretion. The timing, content, manner of effectuating and party to execute provision of any notices will be determined by SIE in its sole discretion. Except as required by law, in no event will Vendor serve any notice of, inform a third party of, or otherwise publicize the Information Security Incident, without the prior written consent of SIE.

4.5. If Vendor fails to comply with the obligations set forth in this Section 4, SIE will be entitled to, at SIE's sole discretion, to immediately suspend Processing of SIE Data or access to SIE Systems until the suspension-related issue is resolved or terminate the Agreement with immediate effect and without liability to SIE.

5. **Security Assessment.** Vendor represents and warrants to SIE that it has completed any information security questionnaire(s) (the "**Questionnaires**") provided to Vendor by SIE and Vendor's responses to the Questionnaires are accurate as of the date of the Questionnaires. Vendor acknowledges and agrees that upon completion of any Questionnaires, SIE may require additional information to complete the SIE Security Assessment (the "**Assessment**"), and Vendor will comply with all requests for such information. If, with respect to the Assessment, SIE identifies any vulnerabilities or security issues that SIE categorizes as a temporal score of 2.0 or above using CVSS (or is Level 2 or above using SVSR), Vendor will (if it has not already done so prior to the date of this Security Rider), take immediate corrective action after the date of this Security Rider to SIE's reasonable satisfaction. If Vendor fails to correct such issues within ten (10) business days or provide SIE with a plan for corrective action within ten (10) business days, including a target date to implement the corrective action that is approved by SIE, SIE will be entitled, at SIE's sole discretion, to immediately suspend access to SIE Systems, SIE Data, or terminate the Agreement upon written notice to Vendor and without liability. In the event that SIE elects to suspend, such suspension shall continue until Vendor resolves such suspension-related issues to SIE's satisfaction (which shall be at SIE's sole discretion). With respect to the Questionnaire and Assessment, other vulnerabilities identified by SIE and categorized by it as being below the temporal score of 2.0 using CVSS or Level 2 using SVSR will be corrected by the Vendor within a reasonable time.

## 6. Information to be Provided.

6.1. **Controls Report.** Upon SIE's request or within forty five (45) days of completion, whichever is sooner, once per year or as frequently as obtained by Vendor, Vendor will provide SIE with reports created by an appropriately credited and objective third party at Vendor's own expense regarding Vendor's security controls for Vendor Systems or that are otherwise relevant to the security of SIE Data or SIE Systems and any failure to meet control objectives required by the applicable standard (for example, SOC 2, ISO27001, NIST 800-53, PCI DSS, IASME, BITS AUP, MPAA, CDSA or similar reports, each a, "**Controls Report**"). If Vendor refuses to provide such Controls Report, SIE may appoint a qualified audit firm to perform the review and prepare the Controls Report, at Vendor's expense.

6.2. **Right to Audit.** SIE, or its designee, will have the right upon five (5) days' prior written notice to enter any premises where the Services, or any part thereof, are performed, for the purpose of confirming that the Information Security Program is consistent with terms herein and whether the Information Security Program has been adequately implemented to ensure the security of SIE Data. During any such audit or inspection, Vendor will (and will cause its affiliates and its and their agents and contractors to) provide SIE, or its designee, access: (a) to observe the operations of Vendor (and its affiliates, and its and their agents and contractors) and to interview their respective relevant personnel in connection with the Services, and (b) to all records, in whatever form maintained, relating to the provision of the Services, and access to all Vendor Systems used by Vendor (its affiliates, or its or their agents or contractors) in performing the Services, as reasonably necessary.



Such records will include, without limitation, the results of tests and audits conducted in accordance with this Exhibit. In the event that such audit discovers an issue or vulnerability, SIE will be entitled to, at SIE's sole discretion, immediately suspend access to SIE Systems or terminate the Agreement upon written notice to Vendor and without liability. In the event that SIE elects to suspend, such suspension shall continue until Vendor resolves such suspension-related issues to SIE's satisfaction (which shall be at SIE's sole discretion).

- 6.3. Remediation Requirements.** Vendor shall remediate all issues identified by a Controls Report, Vendor's Information Security Program, Information Security Assessment, or as otherwise identified by SIE pursuant to an audit. In the event that applicable and/or sufficient remediation is not addressed in the Controls Report, Vendor will (a) prepare within thirty (30) days a timely remediation action plan to correct any deficiencies and/or resolve any problems identified in such Controls Report, provided that such corrective action plan is discussed with and approved in advance by SIE, and (b) Vendor will promptly correct to SIE's satisfaction, any such vulnerability or security issue. Costs of such remediation shall be borne by the Vendor. If Vendor fails to do so, SIE will have the right to terminate the Agreement immediately upon written notice to Vendor and without liability.
- 7. Acceptable Use Policy.** If Vendor personnel will have access to or use of SIE's Systems, the terms and conditions of SIE's Acceptable Use Policy set forth in Attachment 1 to this Schedule 1 (including as amended and provided by SIE from time-to-time in its sole discretion) will also be applicable to Vendor and each of its personnel having such access or use.
- 8. Sub-Contractors.** To the extent Vendor may engage any other party to Process SIE Data or perform the Services and that party has not otherwise been approved as a Subprocessor under Section 3 of the Privacy Rider and disclosed in Schedule 2 above (i.e., because the other party does not Process SIE Personal Information) (a "**Sub-Contractor**"), Vendor shall:
- 8.1.** Bind the Sub-Contractor in a written agreement with Vendor that includes confidentiality and security obligations no less protective than those contained in this Schedule 1;
  - 8.2.** Remain fully liable to SIE for any failure by a Sub-Contractor to fulfil its obligations under Applicable Data Protection Law and this Schedule 1; and,
  - 8.3.** Provide notice to SIE regarding any Sub-Contractors at SIE-Vendor-Notifications@sony.com. Any failure by SIE to object to such notice within thirty (30) days of receipt shall be deemed SIE's authorization to engage such Sub-Contractors.
- 9. System Administrators.** Vendor will comply with the following obligations with respect to any of its personnel performing the role of a system administrator (which for the purposes of this Section shall be deemed to include database administrators, network administrators and any other professional comparable to system administrators) for Vendor Systems: Prior to appointing an individual as such a system administrator, Vendor will assess the candidate's experience, skills, and reliability and seek suitable assurances that the appointment will not cause Vendor to breach any of its obligations to SIE. Vendor will check such system administrators' activities at least annually to verify that they are compliant. Vendor will maintain a list of its personnel who have been appointed as system administrators and include details of the operations that each system administrator can perform, which Vendor shall make to SIE on request.
- 10. PCI-DSS.** To the extent that Vendor Processes any SIE PCI-DSS Data, Vendor acknowledges and agrees that it is responsible for the security of such SIE PCI-DSS Data and will at all times comply with the Payment Card Industry Data Security Standards as well as this Schedule 1. Upon SIE's request, Vendor will provide appropriate attestations or certifications of such compliance.
- 11. Data Retention and Deletion.** Vendor shall not store or make accessible SIE Data for a period longer than required by the purpose of the Agreement. Upon the expiration or termination of the Agreement or SIE's instruction, Vendor will promptly and securely delete or return to SIE any or all SIE Data in all formats. If Vendor is required by law to retain SIE Data, Vendor shall inform SIE of which SIE Data is to be retained, for what purpose, and the period for which it will be retained. The deletion or destruction of SIE Data, whether in electronic or physical form, shall be a sufficiently

secure method that ensures the data cannot be read or reconstructed, and in accordance with SIE's reasonable directions (if any). Vendor shall provide SIE with a written confirmation of such return or destruction.

**Attachment 1 to Information Security Rider**  
*(if applicable)*

**ACCEPTABLE USE POLICY**

If Vendor shall have access to or use of SIE's internal information technology systems, Vendor and Vendor's employees, consultants and agents (together "Contractors") must comply with the following SIE communication policy regarding access to and use of such systems, which include without limitation:

- A. E-mail
  - B. Computer hardware
  - C. Computer software
  - D. Computer databases
  - E. Software applications including web accessed applications
  - F. Telephone, voicemail, and facsimile
1. Monitoring and Reporting. SIE, or another party authorized by SIE, may monitor and conduct audits of SIE information technology systems and may, at any time, examine all data stored or Processed in any of such systems without any prior notification to ensure compliance with this policy. Violations of this policy may result in, among other things, immediate termination of the Agreement by SIE without penalty.
  2. Internet (Web) Usage. Internet and intranet access is provided as a tool to be used for SIE official business. Unauthorized and inappropriate use is prohibited, including without limitation usage for any purpose not directly related to the person's specific job function, and access of websites that contain information that may be considered offensive, as determined by SIE, such as retrieval, access, or downloading of materials which are sexually explicit, profane, or pornographic, and those which pertain to racism and hate.
  3. Email, Telephone, Voicemail, and Facsimile Usage. Email, telephone, voicemail and facsimile are provided for business purposes only. Inappropriate use of such systems is prohibited, including without limitation usage for any purpose not directly related to Contractor's job function, and creation, access, download, or distribution of emails or data that SIE determines to be offensive such as:
    - 3.1. Vulgarities or obscenities
    - 3.2. Sexual comments or images
    - 3.3. Racial slurs
    - 3.4. Gender-specific comments
    - 3.5. Any other comments that could be considered harassing, threatening, discriminatory, or offensive, including without limitation based upon gender, age, race, sexual orientation, religious or political beliefs, ethnic origin, or disability.
  4. User ID and Password Administration. Contractors must obtain unique user identification ("User ID") and passwords from SIE. Access to SIE systems shall not be granted until such User IDs and passwords are issued. Only SIE-designated managers can request User IDs and passwords on behalf of Contractors. Contractors must ensure that User IDs and passwords are kept confidential. Sharing of User IDs and passwords or use for purposes outside of those for which they have been issued is strictly prohibited. Contractors must immediately notify their manager if they have reason to believe that their User ID or password is compromised.
  5. Access and Control. Contractors are responsible for taking appropriate actions to protect SIE systems and information from unauthorized use and disclosure and are prohibited from:
    - 5.1. Downloading, installing, or running security programs or utilities which might reveal weaknesses in the security of SIE's systems unless a job specifically requires it.
    - 5.2. Using SIE's systems and User IDs without authorization or for purposes other than those for which they were intended or authorized.
    - 5.3. Attempting to modify, install, or remove computer equipment, software, or peripherals without proper authorization. This includes installing any non-work related software on SIE-owned equipment.
    - 5.4. Circumventing or attempting to circumvent normal resource limits, logon procedures, or security regulations.
    - 5.5. Sending fraudulent email, breaking into another user's email box, or reading someone else's email without his or her permission.

- 5.6. Sending any fraudulent electronic transmission, including, but not limited to, fraudulent requests for Confidential Information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.
- 5.7. Violating any software license agreement or copyright, including using, copying, or redistributing copyrighted computer software, data, or reports without proper authorization.
- 5.8. Modifying system facilities, operating systems or disk partitions without authorization; attempting to crash or tie up a SIE computer, or damaging or vandalizing SIE computing facilities, equipment, software, or computer files.
- 5.9. Disclosing or removing proprietary information, software, printed output, or magnetic media without SIE's explicit permission.
- 5.10. Reading other users' data, information, files or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.
- 5.11. Creating or transmitting to fellow employees, clients, or customers any chain letters, personal business ads, solicitations, promotions, or commercial announcements.
- 5.12. Creating, transmitting, viewing, using, or storing "pirated" software or any communication, data or information which is in violation of another person's legal, proprietary or trade secret rights.
- 5.13. Creating, transmitting, viewing, using or storing destructive software code or programming (e.g., viruses, Trojan horse programs, etc.).
- 5.14. Creating, transmitting, viewing, using or storing any unauthorized communication, data, or information, or otherwise making public or disseminating any unauthorized message or transmission relating to SIE, its business, products, finances or competitors, or containing any confidential or trade secret information.
6. Network Equipment and Software. Contractors must use desktop, laptop, and other network equipment and software that have been approved and configured by SIE information technology support personnel. No third-party equipment or software may be connected to or installed on the SIE network without prior written approval by SIE information technology support personnel. Unauthorized software and devices may be disconnected or uninstalled by SIE without notice.
7. Transmission of Confidential Information. Confidential Information must never be transmitted over a network without appropriate protection. Appropriate encryption technology must be applied through prior coordination with SIE information technology support personnel or other persons designated by SIE. Furthermore, communications sent via SIE's systems must not disclose any Confidential Information of SIE or any third-party confidential information that has been entrusted to SIE unless a SIE law department-approved nondisclosure agreement covering such Confidential Information has been executed by the applicable parties. All SIE developed software, procedures, and business practices are considered confidential and protected and shall not be shared outside SIE without proper authorization.
8. Access Controls. Before any protected information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with the necessary access controls applicable to the information. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred. In particular, copying protected information from a secure source to an unsecured location on the network is prohibited.
9. Expectation of Privacy. All messages and data files stored on or sent over SIE systems are the property of SIE. SIE provides access to SIE systems for business purposes and to help users to communicate. Subject to applicable privacy laws, SIE will monitor the SIE systems and may in some circumstances retrieve communications. It is not recommended that individuals use the SIE systems for personal use. Any data a person does not want disclosed to SIE should not be transmitted, received, or stored on SIE systems.
10. Remote Access. Remote access to SIE systems requires separate, specific authorization. Only SIE employees with business needs are eligible for remotely accessing SIE's network via remote access. Contractors are not permitted to access the SIE network from a non-SIE site using remote access without written approval from a SIE information technology support senior manager level or above. Individuals who are granted remote access to the SIE network must adhere to all applicable corporate policies, standards, guidelines, and procedures.
11. Global Information Security Standards. All Contractors shall be required to complete SIE security training and acknowledge that they shall abide by these policies and the then-applicable SIE Global Information Security Standards. Vendor can review these standards by contacting SIE.