Spreedly Partner GDPR Annex
Compliance with the EU General Data Protection Regulation

Spreedly, Inc. (the "Processor") and the company to whom this GDPR Annex ("DPA") has been sent (the "Controller") have one or more written agreements (collectively, "the Agreements") pursuant to which the Processor provides services to the Controller (collectively, the "Services") that may entail the Processing of Personal Data (as defined below).

The European General Data Protection Regulation (GDPR) imposes specific obligations on controllers and processors with regard to their vendor relationships. The GDPR requires companies to conduct appropriate due diligence and to have contracts containing specific provisions relating to data protection.

Each of the Agreements contains provisions requiring each party to comply with all applicable laws. This DPA documents the data protection requirements imposed upon the parties by the GDPR. To the extent applicable, this DPA is hereby incorporated by reference into each Agreement in order to demonstrate the parties' compliance with the GDPR.

1. For purposes of this Annex the term "GDPR" shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 or (as applicable) Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"), and any additional implementing legislation, rules or regulations that are issued by applicable supervisory authorities pertaining to data privacy, data security and/or the protection of Personal Data. Words and phrases in this Annex shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR (or the UK GDPR, as applicable). In particular:

   (a) "Controller' has the meaning given to it in Article 4(7) of the GDPR: "means the natural of legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

   (b) "Personal Data" has the meaning given to it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," but only to the extent such personal data pertains to residents of the European Economic Area (EEA) or the UK or are otherwise subject to the GDPR.

   (c) "Personal Data Breach" has the meaning given to it in Article 4(12) of the GDPR: "[any] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

   (d) "Processing" has the meaning given to it in Article 4(2) of the GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

   (e) "Subprocessor" means any processor as defined in Article 4(8) of the GDPR: "[any] natural or legal person, public authority, agency or other body which processes personal data" on behalf of the Processor (including any affiliate of the Processor).

   (f) "Transfer" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means. Transfer also includes moving the Personal Data within a single party from an EU member State (or the UK as applicable) to a country not within the EU (or to a country outside the UK as applicable), or otherwise making such data accessible outside the EU (or the UK as applicable).

(g) "Approved Jurisdiction" means a jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

(h) "Standard Contractual Clauses" means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the European Council (available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted by the European Commission Decision 2004/915: Commission Decision of 27 December 2004 amending Decision 2001/497/EC

2. In accordance with GDPR Article 28(1), Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its Processing of Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

3. The Processor shall not subcontract its obligations under this DPA to another person or entity ("Sub-processor(s)"), in whole or in part, other than the Sub-processors detailed in list of Subprocessors used throughout the service (updated to the signing date of this DPA), including the Subprocessor's name and purpose of their processing. This list will be maintained up to date and accessible via http://www.spreedly.com/gdpr/subprocessors. Controllers may receive notifications of any addition/replacement of other Subprocessors by emailing subprocessor@spreedly.com with the subject "Subscribe" and once subscribed in this manner that Controller will receive notification of such Subprocessors before those Subprocessors are authorized to process Personal Data on behalf of the Processor.

   (a) The controller may reasonably object to the Processor's use of new a Subprocessor by notifying the Processor in writing within ten business days of receiving the notice of intent to authorize via the mechanism specified in Section 3 above. This notice shall explain the reasonable grounds for objection (e.g., if the use of this Subprocessor would violate applicable laws or weaken protections for the applicable Personal Data). The Processor will make commercially reasonable efforts to resolve the objection by the Controller. If the Processor is unable to resolve the objection within a reasonable period of time, not to exceed 30 days, then either party may terminate the agreements without penalty.

   (b) The Processor will execute a written agreement with such approved Sub-processor containing terms providing at least equivalent protection of Personal Data as provided under this DPA (provided that Processor shall not be entitled to permit the Sub-processor to further sub-process or otherwise delegate all or any part of the Sub-processor's processing without Controller's prior written consent at Controller's sole discretion) and which expressly provides the Controller with third party beneficiary rights to enforce such terms and/or require the Processor to procure that the Sub-processor enters into a data processing agreement with Controller directly.

   (c) The Processor shall ensure that each Sub-processor is contractually obligated to perform, and actively performs all applicable obligations under the GDPR as a Processor, as if it were party to this DPA in place of the Processor. Further, the Processor shall ensure that any Sub-processor is required to abide by the same level of data protection, security and confidentiality as the Processor under this DPA and/or the GDPR.

   (d) The Processor shall be liable for the acts or omissions of Sub-processors to the same extent it is liable for its own actions or omissions under this DPA and/or the GDPR.

4. In accordance with GDPR Article 28(3), the following terms are incorporated by reference into the Agreements:

   (a) The Processor shall only process the Personal Data (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from the Controller, including with regard to any Transfers, and (iii) as

needed to comply with law (in which case, the Processor shall provide prior notice to the Controller of such legal requirement, unless that law prohibits this disclosure);

(b) Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) Processor shall take all security measures required by GDPR Article 32, namely:

i. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

ii. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

iii. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process such Personal Data except upon instructions from the Controller, unless the Processor is required to do so by EEA Member State law.

(d) Taking into account the nature of the processing, Processor shall reasonably assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights;

(e) Taking into account the nature of processing and the information available to the Processor, Processor shall comply with (and shall reasonably assist the Controller to comply with) the obligations regarding Personal Data Breaches (as set forth in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as set forth in GDPR Article 36);

(f) At the Controller's discretion, the Processor shall delete or return all the Personal Data to the Controller after the end of the provision of services relating to Processing or upon the Controller's written request at any time during the term of the Agreements, and delete existing copies and procure the deletion of all copies of Personal Data in the possession of its Sub-processors unless applicable EEA member state law requires storage of the Personal Data. The terms of this DPA shall remain applicable to the processing of such Personal Data until returned or erased. At the Controller's request, the Processor shall give the Controller a certificate confirming that it, and each of his Sub-processors, has fully complied with the requirements of this clause;

(g) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller; and

(h) The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

5. The Processor shall provide full, reasonable cooperation and assistance to the Controller in:

(a) upon receipt of: (a) requests from Data Subjects to exercise their rights under the GDPR in connection with Personal Data processed under this DPA, including (without limitation) the right of access, right to rectification,

restriction of processing, erasure, data portability, object to the processing, or the right not to be subject to an automated individual decision making; and/or (b) any requests or inquiries from supervisory authorities, customers, or others, to provide information related to Processor's processing of Personal Data under this DPA; shall: (i) direct such requests to the Controller without undue delay, and (ii) not respond or act upon such requests without prior written approval from The Controller and in accordance with its instructions; and (iii) promptly, and in any case within the period of time required in GDPR, provide full, reasonable cooperation and assistance to the Controller responding to and exercising such requests, except where the foregoing shall not apply only and insofar as it conflicts with GDPR.

(b) ensuring compliance with any notification obligations regarding Personal Data Breach to the supervisory authority and communication obligations to Data Subjects, as required under GDPR.

6. The Processor shall not Transfer any Personal Data (and shall not permit its Sub-processors to Transfer any Personal Data) without the prior consent of the Controller. The Processor understands that the Controller must approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the Transfer exists.

   (a) Where the GDPR is applicable, to the extent Processor's Sub-processor processes Personal Data outside the EEA or an Approved Jurisdiction, such transfer shall be based on one of the appropriate safeguards specified in Article 46 of the GDPR.

   (b) If the transfer of Personal Data is Subject to the GPDR and Processor and/or its Sub-processors intend to rely on Standard Contractual Clauses (where subcontracting or performance is allowed by the Agreements), then the Parties shall be deemed to enter into the Standard Contractual Clauses, subject to any amendments contained in Schedule A. If the Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the new or modified Standard Contractual Clauses shall be deemed to be incorporated into this DPA, and the Processor will promptly begin complying with such Standard Contractual Clauses. The Processor will abide by the obligations set forth under the Standard Contractual Clauses for data importer and/or Sub-processor as the case may be.

7. The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will notify The Controller in writing without undue delay and in any event, no later than 24 hours after becoming aware of an event of any Personal Data Breach.

   (a) The foregoing notification shall include, at least: (a) the nature of the Personal Data Breach incident, where possible, the categories and approximate numbers of Data Subjects concerned, and the categories and approximate numbers of Personal Data records concerned; (b) communicate the name and contact details of the Processor's DPO or other relevant contact from whom more information may be obtained; (c) describe the likely consequences of the Personal Data Breach incident; and (d) describe the measures taken or proposed to be taken to address the Personal Data Breach incident;

   (b) The Processor shall execute thorough investigation and co-operate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach incident.

8. The Processor shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for the Controller) Processor shall make them available to the Controller upon request.

9. The Processor will allow the Controller, or a third-party appointed by the Controller, to conduct audits (including inspections) to verify the Processor's compliance with the Agreements described in this document.

   (a) The Controller may request an audit by emailing success@spreedly.com.

   (b) Following receipt of this request, the Processor and Controller will discuss and agree in advance on the reasonable

scope, start date and duration of this audit, as well as any applicable security and confidentiality controls that may be required.

(c) The Controller will be responsible for any fees charged by any third-party auditor appointed by the Controller for this audit.

10. In Accordance with GDPR Article 24(1), the following terms are incorporated by reference into the Agreements:

Controller and Processor acknowledge that the Controller may engage a third-party payment gateway service provider and/or a third-party payment processing service provider to facilitate payment transactions in connection with the Agreements ("Third Party Gateway or Payment Service"). Any such Third Party Gateway or Payment Service engaged by the Controller shall not be deemed a Subprocessor of the Processor for purposes of this DPA. Accordingly, nothing in this DPA obligates the Processor to enter into a data protection agreement with such Third Party Gateway or Payment Service or to be responsible or liable for such Third Party Gateway or Payment Provider's acts or omissions.

11. No changes, modifications or amendments to this DPA shall be valid or binding unless made in writing and signed by both Parties.

12. In the event and to the extent that the GDPR impose stricter obligations on the Parties than under this DPA, the GDPR shall prevail.

IN WITNESS WHEREOF, authorized representatives of the parties have executed this Agreement as of the last date of signature below:

Spreedly, Inc.

By: DocuSigned by: Jennifer Rosario 3B9BAAB72AE947E...
Name: Jennifer Rosario
Title: CISO
Date: 1/10/2022

Customer

By: Plus 500 Ltd
Name: David Zruia Elad Even-Chen
Title: CEO CFO
Date: 9/11/22 9/11/22

Plus500 Ltd.
פלוס500 בע"מ
514142140

Schedule A – Standard Contractual Clauses Stipulations

1. This Schedule A sets out the Parties' agreed interpretation of their respective obligations under the Controller to Processor Standard Contractual Clauses (Module 2), or under the UK Standard Contractual Clauses (as applicable).

2. Where the transfer of Personal Data is subject to the EU GDPR and the transfer relies on the Standard Contractual Clauses, then the following amendments shall apply to the Standard Contractual Clauses:

   2.1. The Parties agree that for the purpose of transfer of Personal Data between the Controller (Data Exporter) and the Processor (Data Importer), the following shall apply:

   2.1.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.
   2.1.2. In Clause 9, option 1 shall apply. The Data Importer shall submit the request for specific authorization at least thirty (30) days prior to the engagement of the Sub-processor. The Data Importer's sub-processors list shall be updated accordingly.
   2.1.3. In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
   2.1.4. In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Ireland.
   2.1.5. In Clause 18(b) the Parties choose the courts of Dublin, Ireland as their choice of forum and jurisdiction.

3. Where the transfer of Personal Data is subject to the UK GDPR and the transfer relies on the UK Standard Contractual Clauses, then the following amendments shall apply to the UK Standard Contractual Clauses:
   3.1. The supervisory authority shall be the Information Commissioner's Office.
   3.2. The laws of England and Wales shall govern the UK Standard Contractual Clauses.
   3.3. The Parties choose the English courts as their choice of forum and jurisdiction.
   3.4. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK".

4. The Parties shall complete Annex I-II below, which are incorporated in the Standard Contractual Clauses by reference.

Annex I – Description of processing activities

Identification of Parties
"Data Exporter": Plus500 Ltd.;
"Data Importer": the Processor.

Description of Transfer:

a. Categories of Data Subjects: Plus500's customers.
b. Categories of data: Financial identification data, PII
c. Special Categories of Data: N/A
d. The frequency of the transfer: Continuous
e. Nature of the processing: Recording, Disclosure, dissemination or otherwise making available and Erasure or destruction of Plus500 Ltd.'s customers' personal data.
f. Purpose of the transfer and further processing: As defined in the Agreements.
g. Retention period: Personal Data will be retained for the term of the Agreements.
h. Competent Supervisory Authority: The competent supervisory authority shall be set in accordance with the provisions of Clause 13 of the Standard Contractual Clauses. Notwithstanding the foregoing, to the extent that the transfer of Personal Data is subject to the UK GDPR, then the competent supervisory authority shall be the Information Commissioner's Office.

Annex II – Technical and Organizational Measures to Ensure the Security of the Data

Security Controls	
Information Security Governance	A comprehensive information security program including a policy written in one or more readily accessible parts that: (1) contains technical, physical, administrative and procedural controls to provide for the security, confidentiality, integrity and availability of Information and Supplier Systems; (2) protect against hazards or threats and unauthorized access or use of Information; (3) controls identified risks; (4) addresses access, retention and transport of Information, and (5) acceptable use. Designate an individual to manage and coordinate its written security policy and who is sufficiently trained, qualified and experienced to be able to fulfill those functions and any other functions that might reasonably be expected to be carried out by the individual as a security manager or officer.
Asset Management	Mechanisms exist to inventory system components that: (1) Accurately reflects the current system; (2) Is at the level of granularity deemed necessary for tracking and reporting; and (3) Includes organization-defined information deemed necessary to achieve effective property accountability. All corporate laptops are full disk encrypted and wiped per industry standards when decommissioned. All infrastructure equipment housing Personal Data resides within certified third-party data centers within AWS. AWS currently uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.
Business Continuity and Disaster Recovery	Plans and regular exercises to address business continuity of key people and processes along with disaster recovery plans for critical technology resiliency.
Change Management	Mechanisms exist to govern the technical configuration change control processes. Prior to implementing changes to the Spreedly platform Spreedly will assess the potential impact of such changes on Security and determine whether such changes are consistent with existing Security. No changes to the Spreedly platform or Security should be made which increase the risk of a Personal Data Breach or which would reduce the controls of this Annex.
Cloud Security	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.
Compliance	Mechanisms exist to facilitate the identification and implementation of relevant legislative statutory, regulatory, and contractual controls.
Configuration Management	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.
Continuous logging and monitoring	Mechanisms exist to ensure that all systems used to store Personal Data are logged, monitored, and reviewed regularly.
Cryptographic Protections	Spreedly will encrypt all sensitive cardholder data using appropriate encryption technology wherever it is stored or transmitted. Spreedly will use only strong, public encryption algorithms and reputable cryptographic implementations and will not employ any proprietary cryptography.
Data Classification and Handling	Mechanisms exist to facilitate the implementation of data protection controls to ensure data and assets are categorized in accordance with applicable statutory, regulatory, and contractual requirements.

Endpoint Security	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices including but not limited to (1) utilization of anti-malware technologies to detect and eradicate malicious code; (2) automatic updates of anti-malware technologies, including signature definitions; (3) ensuring that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period; and (4) utilization of host-based firewall software, or a similar technology, on all information systems, where technically feasible.
HR Security	As permitted by applicable Law, conduct reasonable background checks of any Spreedly personnel that will have access to Personal Data, including Criminal Record Bureau checks. Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.
Identification and Authentication	Mechanisms exist to (1) provide physical access controls, secure user authentication protocols, secure access control methods, and firewall protection; and (2) prevent terminated Supplier Personnel from accessing Information and Supplier Systems by promptly terminating their physical and electronic access to such Information. With respect to Supplier Systems and Information: (1) maintain secure control over user IDs, passwords and other authentication identifiers; (2) maintain a secure method for selecting and assigning passwords and using authentication technologies such as token devices; (3) Restrict access to only active users/accounts; (4) block user access after multiple unsuccessful attempts to login or otherwise gain access; (5) assign unique user identifications plus passwords, which are not vendor supplied default passwords; and (6) require personnel to change passwords at regular intervals and whenever there is any indication of possible system or password compromise, and avoid re-using or cycling old passwords. Duties and areas of responsibility of Supplier Personnel are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Supplier System or Information.
Incident Response	Maintain policies and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and encouraging reporting actual or reasonably suspected Personal Data Breaches, including: (1) training Supplier's personnel with access to Personal Data to recognize actual or potential Personal Data Breaches and to escalate and notify the senior management of the foregoing; (2) mandatory post-incident review of events and actions taken concerning security of Personal Data.
Malicious Code Mitigation Software	Mechanisms exist to (1) implement and maintain software for Spreedly systems that detects, protects against, removes and remedies software or computer code designed to perform an unauthorized function on, or permit unauthorized access to, an information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs; (2) run mitigation software on at least a weekly basis; (3) update mitigation software automatically, including without limitation, obtaining and implementing the most currently available virus signatures.
Network Security	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network including but not limited to (1) up-to-date firewalls between Supplier System, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks operated by Supplier that are not necessary for providing the Services to Customer, which are reasonably designed to maintain the security of Information and Supplier System; (2) implementation and management of a secure guest network.
Physical and Environmental Security	Mechanisms exist to provide (1) reasonable restrictions on physical access to Personal Data and the Spreedly platform; and (2) physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. Policies concerning security for the storage, access, transportation and destruction of

	records and media containing Information outside of business premises.
Privacy	Mechanisms exist to comply with applicable privacy laws, regulations, and notices.
Risk Management	Periodic and regular information security risk assessment and monitoring of Spreedly's information security program, Security and the Spreedly platform, at least annually, including: (1) identifying and assessing reasonably foreseeable internal and external threats and risks to the security, confidentiality, integrity and availability of Information; (2) assessing the likelihood of, and potential damage that can be caused by, identified threats and risks; (3) regularly testing, monitoring and evaluating the sufficiency and effectiveness of Security and Personal Data Breach response actions, and documenting same; (4) assessing adequacy of Spreedly personnel training concerning, and compliance with, Spreedly's information security program; (5) designing, implementing, adjusting and upgrading Security in order to limit identified threats and risks, and address material changes in technology, business and sensitivity of Personal Data; and (6) assessing whether such information security program is operating in a manner reasonably calculated to prevent unauthorized access or use of Personal Data; and (6) detecting, preventing and responding to attacks, intrusions and other system failures.
Secure Engineering and Architecture	Mechanisms exist to facilitate the implementation of industry-recognized security and privacy practices in the specification, design, development, implementation and modification of systems and services.
Security Awareness and Training	Regular and periodic training of Spreedly personnel concerning: (1) Security; (2) implementing Spreedly 's information security program; and (3) the importance of personal information security.
Technology Development and Acquisition	Spreedly will adhere to industry best practices and standards for Secure Software Development Lifecycle (SSDLC), including all of, but not limited to, the following techniques: (1) Leveraging security guidelines from one or all the following industry best practices and standards – OWASP Top 10, SANS Top 25 and Cloud Security Alliance; (2) Consistently executed secure code reviews and testing either through manual peer review or via a code scanning solution; (3) Protection of test data and content and removal of test data and content before deployment to production; (4) System acceptance testing; and (5) System change control and approvals before deployment to production.
Third Party Management	Mechanisms exist to facilitate the implementation of third-party management controls including but not limited to: (1) reasonable steps and due diligence to select and retain third party suppliers that are capable of maintaining security consistent with this Annex and complying with applicable legal requirements; (2) contractually requiring such suppliers to maintain such security; and (3) regularly assessing and monitoring third party suppliers to confirm their compliance with the applicable security required in this Annex and by law.
Threat Management	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.
Vulnerability and Patch Management	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information including but not limited to (1) software and firmware patching; (2) vulnerability scanning on a recurring basis; and (3) penetration testing conducted by an independent third party twice per year.