# Information Security Addendum – Intel 471 Platform

This Information Security Addendum for Intel 471 Platform ("**Security Addendum**") amends the agreement between Intel 471 and the Customer referencing this Addendum and governing use of Intel 471 Platform ("**Agreement**"). To the extent of any conflict between the Agreement and this Security Addendum with respect to Intel 471 Platform, this Security Addendum shall control.

## Security Program

Intel 471 recognizes that security is a fundamental consideration for Intel 471 Platform customers and maintains a comprehensive documented security program based on SOC 2 requirements, with guidance from NIST security controls, and industry standards and cybersecurity best practices outlined by ISO, under which Intel 471 implements and maintains physical, administrative and technical safeguards designed to protect the confidentiality, integrity, availability and security of Intel 471 Platform and Customer Content (the "**Security Program**") as set forth below. Intel 471 utilizes infrastructure-as-a-service providers (each, a "**Infrastructure Provider**") and provides Intel 471 Platform using storage hosted by the applicable Infrastructure Provider. Intel 471 regularly tests and evaluates its Security Program and may review and update its Security Program as well as this Security Addendum from time to time consistent with industry standards.

## 1. Definitions

**"Customer Content"** means information, data, media or other content provided by Customer (or any users authorized by Customer) for use with Intel 471 Platform.

"**Intel 471 Platform**" means a subscription-based, SaaS offering provided and managed by Intel 471 or its affiliate.

"**Security Incident**" means any unauthorized or unlawful destruction, loss, alteration or access to, or disclosure of, Customer Content that is in Intel 471's possession or under Intel 471's control. It does not include events which are either (i) caused by the Customer or Customer affiliates or their end users or third parties operating under their direction, such as the failure to (a) control user access; (b) secure or encrypt Customer Content which the Customer transmits to and from Intel 471 during performance of the Services; and/or (c) implement security configurations to protect Customer Content; or (ii) unsuccessful attempts or activities that do not or are not reasonably likely to compromise the security of Customer Content, including but not limited to unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

## 2. Audits and Certifications

Intel 471's information security management program used to provide Intel 471 Platform is assessed by independent third-party auditors as described in the following audits and certifications ("**Third Party Audits**"), on an annual basis:

- AICPA SSAE 18 SOC 2 Type 1

## 3. Hosting Location of Customer Content

The hosting location of Customer Content is determined by the location of the production instance of Intel 471 Platform in the United States.

## 4. Encryption

**4.1** **Encryption of Customer Content.** Intel 471 Platform encrypts Customer Content at-rest using AES 256-bit (or better) encryption. Intel 471 Platform uses Transport Layer Security (TLS) 1.2 (or better) for Customer Content in-transit over untrusted networks.

**4.2** **Encryption Key Management.** Intel 471's encryption key management conforms to industry-standards and best practices, and it involves regular rotation of encryption keys. Intel 471 logically separates encryption keys from Customer Content.

## 5. System & Network Security

**5.1** **Access Controls.** Intel 471 Platform is a restricted-view service where Intel 471's internal network and Intel 471 personnel are separate from the production environment. Intel 471 personnel have direct access to Customer's Intel 471 Platform Content on an as-needed basis. The responsibility and access to perform operations, troubleshooting and support activity for Intel 471 Platform is limited and restricted to Intel 471 personnel responsible for site reliability. All Intel 471 personnel access to Intel 471 Platform is via a unique user ID, consistent with the principle of least privilege, requires a VPN, as well as multi-factor authentication and passwords.

**5.2** **Endpoint Controls.** For access to Intel 471 Platform, Intel 471 personnel use Intel 471-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 5.7.3 (Vulnerability Management).

**5.3** **Separation of Environments.** Intel 471 logically separates Intel 471 Platform production environments from development environments.

**5.4** **Firewalls.** Intel 471 shall protect the Intel 471 Platform service using industry standard firewall with deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business-required. In addition, Intel 471 also utilizes WAF technology.

**5.5** **Hardening.** Intel 471 Platform is hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and patching as described in this Security Addendum.

### 5.6 Monitoring & Logging

**5.6.1** **Infrastructure Logs.** Security monitoring tools or services are utilized to log certain activities and changes within Intel 471 Platform. These logs are further monitored, analyzed for anomalies and are securely stored to prevent tampering for at least one year.

**5.6.2** **User Logs.** Audit logs and security logs that are captured within Intel 471's Platform are maintained securely for a minimum of 60 days where they are protected from unauthorized modification and deletion. Information such as session ID, password, and app-specific sensitive data is not captured in any of these logs, including system logs, security logs and application logs within the Platform. These logs are not typically shared with Intel 471 Customers, and the Platform does not support the integration of SIEM tools, where logs can be fed into a third-party security monitoring solution that is used by the Customer. In the event that a security incident were to occur on the Platform that directly impacted a particular Customer, Intel 471 would share the necessary logs with that Customer to support a formal investigation.

### 5.7 Vulnerability Detection & Management

**5.7.1** **Anti-Virus & Vulnerability Detection.** Intel 471 Platform leverages industry standard threat detection tools with daily signature updates, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "**Malicious Code**").

**5.7.2** **Penetration Testing & Vulnerability Detection.** Intel 471 works with an independent third party to conduct penetration tests of Intel 471 Platform at least once annually. Intel 471 also runs monthly vulnerability scans for Intel 471 Platform using updated vulnerability databases.

**5.7.3** **Vulnerability Management.** Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to Intel 471 Platform. To assess whether a vulnerability is 'critical', 'high', or 'medium', Intel 471 leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

## 6. Administrative Controls

**6.1** **Personnel Security.** Intel 471 conducts background checks on Intel 471 personnel as part of our standard hiring process, subject to local laws and regulations.

**6.2** **Personnel Training.** Intel 471 maintains a documented security awareness and training program for Intel 471 personnel that is completed at onboard and annually. Intel 471 personnel are also required to acknowledge and comply with key Intel 471 security policies.

**6.3** **Intel 471 Risk Management & Threat Assessment.** Intel 471's risk management process is based on SOC 2 requirements, with guidance from NIST security controls, and industry standards and cybersecurity best practices outlined by ISO. Intel 471 conducts an annual risk assessment, which includes Intel 471 Platform, to review material changes in the threat environment and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

**6.4** **External Threat Intelligence Monitoring.** In addition to utilizing its own best-in-class threat intelligence, Intel 471 reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 5.7.3 (Vulnerability Management).

**6.5** **Vendor Risk Management.** Intel 471 maintains a vendor risk management program for vendors that process Customer Content designed to ensure each vendor maintains security measures consistent with Intel 471's obligations in this Security Addendum. A list of these subprocessor vendors may be found here.

## 7. Physical & Environmental Controls

**7.1** **Environment Data Centers.** To ensure the Intel 471 Platform Infrastructure Provider has appropriate physical and environmental controls for its data centers hosting the SaaS Service, Intel 471 regularly reviews those controls as audited under the Infrastructure Provider's third-party audits and certifications. Each Infrastructure Provider shall have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks. Such controls, shall include, but are not limited to, the following:

**7.1.1** Physical access to the facilities is controlled at building ingress points;

**7.1.2** Visitors are required to present ID and are signed in;

**7.1.3** Physical access to servers is managed by access control devices;

**7.1.4** Physical access privileges are reviewed regularly;

**7.1.5** Facilities utilize monitor and alarm response procedures;

**7.1.6** Use of CCTV;

**7.1.7** Fire detection and protection systems;

**7.1.8** Power back-up and redundancy systems; and

**7.1.9** Climate control systems.

## 8. Incident Detection & Response

**8.1** **Security Incident**. Upon becoming aware of a Security Incident, Intel 471 will notify the Customer and take reasonable steps to identify, prevent and mitigate the effects of the Security Incident and to remedy the Security Incident to the extent such remediation is within Intel 471's reasonable control.

**8.2** **Investigation.** In the event of a Security Incident as described above, Intel 471 will promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

**8.3** **Communication and Cooperation.** Security Incident notifications, if any, will be delivered to Customer by the means specified in the applicable agreement or, if unspecified, by means selected by Intel 471, including via email. It is the Customer's responsibility to ensure that it provides Intel 471 with accurate contact information and secure transmission at all times. Communications by or on behalf of Intel 471 with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Intel 471 of any fault or liability with respect to the Security Incident.

## 9. Business Continuity and Disaster Recovery

**9.1** **Business Continuity Plan/Disaster Recovery Plan.** As it relates to Intel 471 Platform, Intel 471 is prepared to handle large business disruptions with its corporate business continuity program, which is driven by a Business Continuity Policy ("**BC Policy**") and a Business Continuity Plan ("**BCP**"). BCP's are reviewed on an annual basis to confirm they are in accordance with the established policies and procedures. Intel 471 maintains a disaster recovery plan ("**DRP**") to help ensure continued availability. The DRP is tested at least annually. Data backups are managed by an Infrastructure Provider to ensure redundancy. Primary and secondary backups are daily incremental and are encrypted in transit (SSL/TLS 1.2) and at rest (AES-256). Backups are retained in accordance with Intel 471's internal Data Deletion Policy.

## 10. Deletion of Customer Content

**10.1** **By Customer.** Intel 471 Platform provides Customer controls for the deletion of Customer Content.

**10.2** **By Intel 471.** Subject to applicable provisions of the Agreement and deletion of primary data by Customer, upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "**retrieval period**" set forth in the Agreement, Intel 471 shall regularly delete backups of Customer Content in accordance with its internal Data Deletion Policy.

## 11. Customer Rights & Shared Security Responsibilities

**11.1** **Customer Audit and Inquiry Rights**.

**11.1.1** Upon written request and at no additional cost to Customer, Intel 471 shall provide Customer, and/or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Intel 471's compliance with its obligations under this Security Addendum in the form of, as applicable, (i) Intel 471's SOC 2 Type I audit report (ii) Intel 471's most recently completed industry standard security questionnaire, such as a SIG or CAIQ, and (iii) architecture and technical overview documentation for the Service (collectively, "**Audit Reports**"). Audit Reports are considered Intel 471's Confidential Information.

**11.2** **Shared Security Responsibilities.** Without diminishing Intel 471's commitments in this Security Addendum, Customer agrees:

**11.2.1** Intel 471 has no obligation to assess the content or accuracy of Customer Content, including to identify information subject to any specific legal, regulatory or other requirement.

**11.2.2** Customer is responsible for managing and protecting its user roles and credentials, including but not limited to (i) ensuring that all users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to Intel 471 any suspicious activities related to Customer's account (e.g., a user credential has been compromised), and (iii) maintaining appropriate authentication, password and logging controls.

**11.2.3** Customer is responsible for the security of any and all third-party software or applications installed and utilized by the Customer in conjunction with Intel 471 Platform.