

SECURITY ADDENDUM

Last Updated: Feb. 2026

This Security Addendum is part of and incorporated into the Terms of Service located at <https://connect.na.panasonic.com/terms-conditions-sale> (or such successor URL as may be designated by PCNA) (the “**Terms**”) and shall be effective and remain in force for so long as PCNA continues to provide the Cloud Platform to Customer.

1. **DEFINITIONS.** Capitalized terms not defined in this Security Addendum are defined in the Terms. In the event of any conflict between the body of this Security Addendum and the Terms, this Security Addendum shall govern.

1.1. “**Encryption**” shall mean the process or method of encoding information into an unrecognizable form using a publicly available algorithm designed to prevent an unauthorized recipient from understanding or recognizing the original, unencoded information without the use of a key or password.

1.2. “**Security Incident**” shall mean (a) the unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to, Customer Data, or (b) a violation of any international, foreign, federal, state, and local laws, statutes, rules, orders, and regulations related to data security or privacy applicable to the Customer Data in PCNA’s possession or control.

2. **INFORMATION SECURITY**

2.1 **Procedures and Safeguards.** PCNA will establish and maintain physical, technical, and administrative safeguards against the malicious or unauthorized access, acquisition, disclosure, destruction, corruption, loss, misuse, alteration, or other interference of Customer Data that are: (a) no less rigorous than those maintained by PCNA for its own information or the information of its customers of a similar nature; and (b) no less rigorous than the accepted practices in the industry.

2.2 **Physical Security.** PCNA shall house or cause its cloud provider to house the Cloud Platform in physically secure premises protected at least by fire and flood protection and access-controlled doors. In addition, PCNA shall utilize industry-standard and up-to-date firewalls and intrusion checking and/or protection software and/or equipment.

2.3 **Encryption**

(a) Upon request, PCNA shall provide end-to-end Encryption for electronic communications (i.e. email) between PCNA and Customer (including their respective employees, contractors, or outsourcers) while exchanging any Customer Data.

(b) PCNA shall use end-to-end Encryption for any Customer Data received by the Cloud Platform that is transmitted or received over any data communications network or network technology that may be reasonably eavesdropped by a third party, including any transmission or reception over the public internet or through the use of any wireless technology.

- (c) PCNA shall use Encryption for all Customer Data at rest while stored on the Cloud Platform.
- (d) All non-public key material (including symmetric keys) used for Encryption shall be stored in a manner reasonably designed to protect the confidentiality, integrity, and availability of such keys.

2.4 PCNA's Network Security System. PCNA shall establish and maintain a security system covering the Cloud Platform. At a minimum the security system will include the following elements:

- (a) appropriate levels of controls for granting access to source code, data, graphics, audio/visual materials and the like used in providing the Cloud Platform. Secure access control measures that include: (i) restrict access to records and files containing Customer Data to those who need such information to perform their job duties; (ii) assign unique identifications plus passwords, which are not PCNA supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls; and (iii) use of two factor identification systems to allow limited and controlled access to PCNA's internal network;
- (b) secure user authentication protocols should comply with current industry best practices and include: (i) control of user IDs and other identifiers; (ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (iii) control of data security passwords to ensure that such passwords are kept in a location and format that does not compromise the security of the data they protect; and (iv) restricting access to current customer's of PCNA and such customer's Authorized Users.
- (c) for any system connected to the Internet, reasonably up-to-date firewall protection and operation system security patches, designed to maintain the confidentiality, integrity and availability of Customer Data; and
- (d) reasonably up-to-date versions of the system security agent software which must include virus and malware protection and reasonably up-to-date patches and virus definitions, and a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis.

2.5 Access to PCNA's Network from External Networks. PCNA agrees that no access from external networks, including the internet, will be permitted unless strong authentication and Encryption is used for such access. PCNA shall maintain an access control list for all access to the internal network from an external network and PCNA agrees that any of its servers exposed to the internet that contain Customer's Confidential Information or Personal Information will run on a hardened operation system.

2.6 Restrict Personnel Access to Records. PCNA shall (a) consider whether and how employees should keep, access and transport records containing Customer Data outside of business premises; and (b) prevent access by terminated employees by immediately terminating their physical and electronic access to such records, including deactivating passwords and user names.

3. DATA SECURITY INCIDENTS

- 3.1 Data Security Incident Notification. PCNA agrees to notify Customer as soon as practicable, but no later than seventy-two (72) hours of PCNA's discovery of a Security Incident. PCNA's notification shall include the name and contact information for at least one member of PCNA's personnel who shall serve as Customer's primary security contact.
- 3.2 Data Security Incident Investigation. At no additional cost, PCNA, to the extent internal resources are available, will use commercially reasonable efforts to cooperate with Customer in investigating the Security Incident, including, but not limited to; (a) conducting forensics reviews of the relevant systems; (b) imaging relevant media; (c) facilitating interviews with PCNA's personnel and others involved in the matter; and (d) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably requested by Customer.
- 3.3 Security Incident Response. On notice of any actual or suspected Security Incident, PCNA will immediately institute appropriate controls to: (a) contain and remedy the Security Incident; (b) prevent any further Security Incidents; (c) comply with all applicable privacy and data security rights, laws, regulations, and standards; and (d) maintain and preserve all electronic evidence relating to the breach in accordance with industry best practices. PCNA shall provide Customer with the documented responsive actions taken in connection with any Security Incident, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Customer Data.
- 3.4 Any information provided under Section 3.2 or Section 3.3 shall be considered the Confidential Information of PCNA.

4. PCNA MONITORING; RISK ASSESSMENTS

- 4.1 PCNA Monitoring. PCNA will regularly monitor its security policies and upgrade the information safeguards as necessary to prevent unauthorized access to or unauthorized use of Customer Data.
- 4.2 Perform Risk Assessments. PCNA shall review the scope of its security measures at least annually or whenever there is a material change in business practices that reasonably implicates the security or integrity of records containing Customer Data. In doing so, PCNA will (a) identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper or other record containing Customer Data; (b) evaluate the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) education and training on the proper use of the computer security system and the importance of information security; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures; and (c) if necessary, improve the safeguards.