FRM-00-03 Acceptable Use Standard

1.0 POLICY

This policy establishes the rules and expectations supporting the proper usage of Peraton IT assets.

2.0 PURPOSE & SCOPE

All computer systems and data residing in the Peraton network infrastructure and environment exist to enable employees and other authorized users to perform work on behalf of the Company and its customers.

This policy applies to Peraton Corporation and its wholly owned subsidiaries (collectively, “Peraton”). This policy defines responsibilities for the protection and appropriate use of Sensitive Information (Peraton Proprietary, Peraton RESTRICTED, Third-Party Proprietary, “Data Classification and Handling”) in electronic or non-electronic formats, that is processed, received, generated, accessed, and transmitted by applications or stored on Peraton IT.

Program Dedicated IT systems, which are dedicated for use by one or more customers and/or delivering services under contracts, will be maintained in compliance with security requirements specified in contracts associated with those systems. Program Dedicated IT systems must, at a minimum, be maintained in compliance with the Peraton corporate security requirements. In the absence of government requirements, Peraton policies and procedures must be followed.

Customer IT is outside the scope of this policy except as it relates to interconnections between Peraton IT and Customer IT.

This policy applies to all Peraton employees, contractors, subcontractors, and system users, regardless of segment/business unit, location, or assignment within the Peraton organization, and all Peraton IT systems and data. Users are defined as anyone with authorized physical and/or electronic access to Peraton IT assets or information including full-time and part-time employees (including permanent, temporary, interns, and on-call/casual employees); outside partners; and any other forms of non- employees. In the absence of government requirements, Peraton policies and procedures must be followed.

Except where otherwise noted, this policy applies to the access and use of Peraton systems and data accessed from any location to include Company facilities, Customer sites, or any remote locations, including but not limited to authorized users’ homes, airports, hotels, and customer facilities. Exceptions to this policy must be reviewed and approved by the Peraton CISO prior to implementation or account access.

Additional restrictions may apply to classified data or programs processed and stored on government- authorized classified and unclassified systems which are subject to additional government-directed security requirements. Peraton facilities having a United States Government (USG) security facility clearance and/or facilities maintaining data that fall under governmental regulatory restrictions will be governed by this policy except where relevant regulations require other or additional procedures.

IT systems and environments, established by companies prior to the acquisition or merger of those companies into Peraton, will be brought into compliance with Peraton IT policies and standards in accordance with the merger/acquisition integration plans. Until such systems are integrated, they will comply with legacy policies definitions.

3.0 DEFINITIONS

3.1 **Controlled Unclassified Information (CUI):** Unclassified information that a U.S. Government agency has labelled CUI per 32 CFR Part 2002. Examples include, but are not limited to, information that has been designated Controlled Unclassified Information (CUI), Controlled Technical Information (CTI), Controlled Unclassified Technical Information (CUTI), and Covered Defense Information (CDI). Access to this information is limited to authorized individuals with a need to know and/or is subject to agency-specific access/dissemination controls (e.g., "NOFORN"
- Information in any form may not be disseminated to foreign governments, foreign nationals, foreign or international organizations, or NON-US citizens).

3.2 **Customer IT:** IT owned or leased by the customer even if Peraton is the purchasing agent or contracted to operate the IT.

3.3 **Enterprise IT:** The interconnected set of Peraton IT resources and services that enable general employee productivity and administrative and support functions.

3.4 **Federal Contract Information (FCI):** Information that is not intended for public release and provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information such as necessary to process payments.

3.5 **Innovation IT:** Any Peraton IT charged to an indirect charge account that is not Enterprise IT. Examples include IT environments or resources established to create proofs of concept, develop a product or offering for **sale, or act as a technology learning space for employees.**

3.6 **Intellectual Property:** Rights arising anywhere in the world under inventions (whether or not patentable or reduced to practice), patents, patent applications, copyrights, trademarks, trade secrets, or other intellectual property, including rights arising under computer software (whether in source or object code form), data and technical data (as such terms are defined in the applicable federal acquisition regulations), hardware, firmware, middleware, mask works and industrial designs, and including all registrations and applications for registration of any of the foregoing, including all renewals, extensions, reissuances, continuations, divisions, or derivative works of any of the foregoing.

3.7 **Peraton IT:** Peraton-owned or -leased hardware, software, and IT services used to store, process, receive, or transmit information. Peraton IT is categorized as Enterprise IT, Program Dedicated IT, or Innovation IT.

3.8 **Personally Identifiable Information (PII):** Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular Data Subject or household: date of birth, a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, biometric data,

geolocation data, and Professional or employment-related information. Unless otherwise required by law, does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity, or information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

3.9 **Program Dedicated IT:** Peraton IT dedicated to a specific program, customer, or set of programs or customers. This includes both billable and unbillable program IT resources.

3.10 **Proprietary Information:** Generally, information maintained as proprietary or confidential by a person or entity and may provide its owner with a business, technological, or economic advantage over its competitors, or which, if known or used by third parties or by the owner's employees or agents in an unauthorized manner, may be detrimental to the owner's commercial interests. Proprietary Information will generally be identified in a Non-Disclosure Agreement ("NDA") or Proprietary Information Agreement ("PIA"). may include, but is not limited to:

a. Existing and contemplated business, marketing, and financial business information such as business plans and methods, marketing information, cost estimates, forecasts, financial data, cost or pricing data, bid and proposal information, customer identification, sources of supply, contemplated product lines, proposed business alliances, and information about customers and competitors.

b. Existing and contemplated technical information and documentation pertaining to technology, know how, equipment, machines, devices and systems, computer hardware and software, compositions, formulas, products, processes, methods, designs, specifications, mask works, testing or evaluation procedures, manufacturing processes, production techniques, research and development activities, inventions, discoveries, and improvements.

3.11 **Sensitive Information:** Data such as Peraton Proprietary, Peraton RESTRICTED, Third-party Proprietary Information, or Information protected under the attorney-client and/or attorney work product privileges or subject to a protective court order, the unauthorized disclosure of which may adversely impact Peraton. Sensitive Information also includes insider threat information, personal information, export-controlled information, and other information designated by the government as requiring special handling and protection. For purposes of this policy, any information not designated as Unrestricted is considered Sensitive Information.

4.0 POLICY REQUIREMENTS

4.1 Peraton systems and data are provided for business purposes only.

4.2 Access to the Peraton systems and data will only be obtained through approved and formal procedures.

4.3 Unless acting on behalf of Peraton during a specific and legitimate, authorized, and approved function, no person obtaining access to Peraton systems and data may intentionally seek to circumvent security controls, exploit vulnerabilities, affect security breaches or disruptions, cause damage or destruction, or share with or use data on other than approved systems.

5.0 POLICY REQUIREMENTS

5.1 Peraton systems and data are provided for business purposes only.

5.2 Access to the Peraton systems and data will only be obtained through approved and formal procedures.

5.3 Unless acting on behalf of Peraton during a specific and legitimate, authorized, and approved function, no person obtaining access to Peraton systems and data may intentionally seek to circumvent security controls, exploit vulnerabilities, affect security breaches or disruptions, cause damage or destruction, or share with or use data on other than approved systems.

5.4 Without authorization from the CISO, it is prohibited for any employee or third-party vendor to use or impersonate Peraton's corporate domains. This includes, but is not limited to, email communications, websites, and/or other online accounts using the Peraton.com domain.

5.5 All workstation screens and computing resources must be locked when devices are unattended for any period of time. If mobile devices are to be left at a Peraton or other authorized facility during off hours, they must be locked away in a secure drawer, cabinet, or room. During transport to or from Peraton facilities, devices must be securely stored (e.g., locked in a car trunk versus left visibly in the car).

5.6 Non-Peraton and/or personal mobile devices (e.g., laptops, tablets, and cellular telephones) are prohibited from accessing Company systems or data and/or being used to perform any functions on a Peraton-managed network or asset unless the approved mobile management solution is utilized to provide Peraton data compartmentalization.

a. If unable to install or utilize the Peraton approved mobile management solution, access to approved apps (e.g., Okta Authenticator, Simpplr, etc.) or hosted software or services via Okta Single Sign-on is permitted. While in use, these assets must adhere to this “Acceptable Use Policy” at all times, and under no circumstances, be used to download corporate or sensitive information.

5.7 Without a granted exception, Peraton-issued computers and other Company devices are prohibited from connecting to customer networks.

5.8 The following requirements apply to all Peraton Proprietary and Sensitive Information, Controlled Unclassified Information (CUI); and Federal Contract Information (FCI) in electronic or non-electronic formats; generated, accessed, transmitted, or stored on devices, systems, and networks.

a. Users are prohibited from disclosing Sensitive Information, CUI, and FCI on any publicly accessible organizational system.
b. User must be officially authorized to access digital (e.g., disks, magnetic tapes, external/removable hard drives, USB, or thumb drives) and non-digital (e.g., paper, microfilm) media containing Sensitive Information, CUI or FCI.
c. To prevent unauthorized disclosure, users must utilize the proper encryption methods when storing, processing, transporting, or transmitting Sensitive Information, CUI, or FCI on digital media, mobile devices, and mobile computing platforms.

d. Users must mark removable media and output containing Sensitive Information, CUI, or FCI indicating the distribution limitations, handling caveats, and applicable security markings.

e. Users must physically control and securely store information asset media containing Sensitive Information, CUI, or FCI within controlled areas using physical security controls and safeguards. Users must protect all media until destroyed or sanitized using approved equipment, techniques, and procedures.

f. Users must protect and control information asset media containing Sensitive Information, CUI, or FCI during transport outside of controlled areas. In addition, Peraton restricts access to such media to authorized personnel who will maintain accountability for this media during transport outside of controlled areas.

5.9 Sharing of login credentials is strictly prohibited. If required, a submitted exception must be reviewed and approved by the Office of the Chief Information Security Officer (OCISO).

5.10 Auto-forwarding of Peraton or customer-related email to other customer, government, company, competitor, or personal email accounts is strictly prohibited, unless authorized by the OCISO and configured by IT.

5.11 The use of email message labeling using tools made available in Outlook is mandatory for all email transmissions using Peraton workstations. Users must classify all email communications (e.g., Unrestricted, Peraton Proprietary, Peraton RESTRICTED) as appropriate based on the classification of the information disseminated. For restricted email transmissions on mobile or web access, users must manually classify email. For additional guidance regarding the labeling of Proprietary and Sensitive Information, please consult SEC-007, “Data Classification and Handling.”

5.12 Only approved software may be installed on or access Peraton systems and data. The Chief Security Officer (CSO) in close coordination with the Chief Information Security Officer (CISO) will maintain procedures for the periodic and case-by-case review of new requests for approved software.

5.13 Network scanning, discovery tools, or network monitoring tools may not be used on any Peraton network unless a proper charter or plan, with the detailed description of the tools, activities, reasoning, and impact is agreed on and authorized by the OCISO.

5.14 The use of external and/or removable storage media (such as thumb drives, external hard drives, scanners, and media burners) to store, process, transport, or transmit Peraton or customer data is strictly prohibited unless encryption is used, or an exception is granted by the OCISO.

5.15 The use of personal or other non-Peraton IT systems to conduct Peraton business is permitted only in the following scenarios:

a. The non-Peraton system is used to access web enabled Peraton applications (in browser mode only) through the Peraton portal (https://sso.peraton.com). Care must be taken to avoid downloading information to the non-Peraton system and information incidentally downloaded must be promptly deleted.

b. The non-Peraton system is used to access a Peraton virtual desktop.

c. The non-Peraton system is enrolled in Peraton’s Mobile Device Management Solution

d. The non-Peraton system is explicitly approved to conduct Peraton business.

All other use of personal or non-Peraton IT systems, cloud services, or personal e-mail to conduct Peraton business is strictly prohibited.

5.16 The use of corporate devices to access personal online cloud storage solutions (i.e., Dropbox, Google Drive, Box, OneDrive, iCloud, etc.), to include personal email and calendar or collaboration accounts or systems (e.g., Google Docs/Drive, iCloud, Gmail, Yahoo Mail, etc.) is strictly prohibited unless an exception is granted by the OCISO.

5.17 Personal online cloud storage solutions including personal email and calendar or collaboration accounts or systems to download, store, process, transport, or transmit Peraton or customer data is strictly prohibited.

5.18 To endure compliance with government acquisition regulations, Peraton personnel are not permitted to have or use the TikTok* application or website on any information technology device (e.g., smartphone, laptop) if the device is required or used to perform work on a federal contract. This prohibition applies to information technology devices, whether owned by the federal government, Peraton, or the employee under the Company's BYOD program.

5.19 Peraton and customer systems and data may not be used in any manner that would be considered inappropriate, unethical, illegal, or in violation of any related Peraton policies and standards, customer requirements, or other external regulations.

Prohibited uses include:

- **a.** Creating, downloading, viewing, storing, copying, or transmitting sexually explicit material.
- **b.** Annoying or harassing another individual through uninvited email or by using lewd or offensive language in email.
- **c.** Creating, copying, transmitting, or retransmitting of chain letters or other unauthorized mass mailings.
- **d.** Using a Peraton computer for commercial purposes or in support of for-profit activities unrelated to Peraton, including outside employment, outside consulting for pay, sales or administration of business transactions, or sale of goods or services.
- **e.** Gambling.
- **f.** Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity unless approved, in advance, by the Peraton Office of General Counsel.
- **g.** Making statements or performing any actions or behaviors that denigrate, deride, disparage, or show hostility or aversion toward an individual or group because of race, color, religion, national origin, sex, age, physical or mental disability, pregnancy, sexual orientation, gender identity, genetic information, veteran status, service in the Uniformed Services of the U.S., or any other protected class under relevant law.
- **h.** Posting Proprietary or Confidential Information to any external newsgroup, chat room, bulletin board, or other public forum without prior approval.
- **i.** Conducting personal activities that could cause congestion, delay, or disruption of service to any office equipment. This includes live streaming of music or videos and sending pictures, video or sound files, or other large file attachments that can degrade computer network performance.
- **j.** Acquiring use, reproduction, transmission, or distribution of any controlled information such as copyrighted computer software, other copyrighted or trademarked material or material with intellectual property rights, privacy

information, and proprietary data.

5.20 Peraton systems and data may not be used for personal use in a way that:

a. Conflicts with the guidelines outlined within this policy or other Company Policies.
b. Is excessive and/or interferes with a user's ability to perform the duties of his/her job.
c. Allows for the use of Company assets by individuals who are not authorized users.
d. Results in incurred costs to the Company including use of telephones, facsimile machines, and voice mail.

5.21 System-specific policies and rules for acceptable use are in addition to and do not replace this policy. All users of Peraton systems and data are personally responsible for following all system- specific policies and rules for acceptable and appropriate use of such systems and data.

5.22 When end-users witness suspicious activity, unexplained anomalies, incidents to include inappropriate use of a computer system, warnings that there may be a threat, or actual data breaches, they must immediately report all issues to the OCISO.

5.23 **Additional Privileged User Account Requirements -** Privileged users are system users and administrators who have been formally authorized and provided with permissions that allow access to systems or data in a manner other than the defined business processes and usage by a typical user of the system or business process. The following statements relate to employees and system users who are granted elevated system or procedural rights.

a. Privileged access to Peraton systems and data will only be obtained through procedures established by the CSO, OCISO, and designated system or data owners.
b. Users who are granted a secondary account to perform administrative tasks will only use those rights while performing functions that require elevated privileges. At all other times, they will login using their regular user accounts.
c. All privileged users will be made aware of and acknowledge their understanding of the unique and exceptional rules for the acceptable use of Peraton systems and data as an integral part of granting privileged access.

END USER ACKNOWLEDGEMENT

By signing, I am acknowledging and agreeing to the following:

- I have read, do understand, and will comply with this policy as a condition of my use of any Peraton systems and data, and if necessary, will seek clarification to ensure complete comprehension and its applicability.
- I understand and agree that Peraton has legal ownership of and authority over the systems and data to which I have been granted access.
- I have no expectation of personal privacy while using or being connected to Peraton systems and data. I also understand that the Company reserves the right to monitor, examine, and audit all systems, data, or services which it operates, provides, or connects, including personal devices I use to access Company systems and data.
- Unless acting on behalf of Peraton during a specific and legitimate, authorized and approved function, I will not intentionally seek to circumvent security controls, exploit vulnerabilities, affect security breaches or disruptions, cause damage or destruction, or share or use data on other than approved systems.
- I will not use another end user's account and/or credentials, or share account credentials assigned to me, with another end user, whether intentionally or through negligence.
- I will not write down or store passwords except in an encrypted, password-protected format.
- I will not transmit Sensitive Information not authorized for public release via unsecure methods such as clear text.
- I will not access, view, send, or store classified information on any unclassified Peraton IT systems or assets.
- Unless authorized, I will not provide corporate email address information to external entities for personal communications or mailing lists unrelated to assigned job duties.
- With the exception of employees, subcontractors, consultants, and customers who acknowledge this policy and are authorized, I will not intentionally allow third-party representatives or vendors to gain access to and/or transfer company or customer information.
- I may not retain Confidential or Sensitive Information after separating from the Company.
- I may not store Sensitive Information on devices not owned or monitored by Peraton except in manners prescribed and authorized by the CSO.
- I will not send any Sensitive Information via text message.
- I will lock my workstation screens and provided systems and accounts when unattended for any period of time. If devices are to be left at a Peraton or other authorized facility during off hours, I will lock them away in a secure drawer, cabinet, or room. During transport to or from Peraton facilities, I will securely store all devices (e.g., locked in a car trunk versus left visibly in the car).
- I will use Peraton systems and data only for their authorized purposes and in accordance with my assigned job duties.
- I will not use portable storage devices when such devices have no identifiable owner.
- I understand that violations of or attempts to circumvent system or data protective measures may be subject to disciplinary action, up to and including termination or legal action.
- I understand that this policy does not release me from complying with other rules and expectations that may be established by law, regulation, customers, or generally accepted ethical behavior.
- I will not knowingly use Peraton systems to violate applicable laws or participate in or access external systems or sites engaged in:
  - Personal business ventures.
  - Business of any other corporation or firm, consulting effort, or similar profit venture.
  - Political interests or political activity, except as provided in the Peraton government relations policy.
  - Illegal drugs or gambling.
  - Pornography and other obscene/sexually explicit materials.
  - Illegal activities and/or information to include violations of export control laws.
  - Defaming or slanderous materials.
  - Violence, bullying/harassment, threatening language.
  - Materials offensive to protected groups (e.g., ethnic slurs, etc.).
  - Malicious code.
  - Non-business-related broadcast messages (e.g., spam, chain letters, advertisements, animated greetings, etc.).
  - Copyright, trade secret, patent, or intellectual property violations (e.g., "pirated" software and files, use of copyrighted software without proper licensing, etc.).

SIGNATURE: _____ **DATE:** _____