Information Security Policy

1. **Purpose and Scope**
    a. This Information Security Policy addresses the information security topics and requirements that maintain the security, confidentiality, integrity, and availability of Perceptyx applications, systems, infrastructure, and data. The topics and requirements addressed in this policy must be continuously improved to maintain a secure information security posture. From time to time, Perceptyx may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to Perceptyx, including compliance with applicable laws and regulations.
    b. This policy applies to all Perceptyx assets utilized by personnel acting on behalf of Perceptyx or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all Perceptyx policies and plans upon onboarding and at least annually thereafter.
        i. Policies are published in Confluence.
            1. Acceptance of this Information Security Policy is an acknowledgment of reading and following all published policies.
    c. This policy clarifies and supersedes the Global Security Policy (GSP). Controls listed in the GSP may be implemented but are not required. For topics not covered here, please reference the GSP for guidance.
2. **Policy**
    a. **Information Security Communication**
        i. Please contact infosec@perceptyx.com if you have any questions about the Perceptyx information security program.
    b. **People Security**
        i. **Background Check**
            1. All Perceptyx personnel are required to complete a background check. An authorized member of Perceptyx must review each background check in accordance with local laws.
        ii. **Confidentiality**
            1. Prior to accessing sensitive information, personnel are required to sign an industry-standard confidentiality agreement protecting Perceptyx confidential information.
        iii. **Security Awareness Training**

1. Perceptyx has a security awareness training program in place to promote the understanding of security policies and procedures. All personnel are required to undergo training following initial employment and annually thereafter. Completion of the training program is recorded and maintained by Perceptyx.

c. **Secure Coding**
    i. Perceptyx promotes the understanding of secure coding to engineers in order to improve the security and robustness of Perceptyx products.
d. **Physical Security**
    i. **Clear Desk**
        1. Perceptyx personnel are required to ensure that all sensitive information in hardcopy or electronic form is secure in their work area when it is unattended. This requirement extends to both remote and in-office work.
        2. Perceptyx personnel must remove hardcopies of sensitive information from desks and lock the information in a drawer when desks are unoccupied and at the end of the work day. Keys used to access sensitive information must not be left at an unattended desk.
    ii. **Clear Screen**
        1. Perceptyx employees and contractors must be aware of their surroundings at all times and ensure that no unauthorized individuals have access to see or hear sensitive information. All mobile and desktop devices must be locked when unoccupied. Session time-outs and lockouts are enforced through technical controls for all systems containing covered information.
        2. All devices containing sensitive information, including mobile devices, shall be configured to automatically lock after a period of inactivity (e.g., screen saver).
e. **Remote Work**
    i. Perceptyx cloud-first architecture allows for employees to work globally; therefore, they must be aware of their responsibilities.
    ii. Any Perceptyx issued devices used to access company applications, systems, infrastructure, or data must be used only by the authorized employee or contractor of such device.

iii. Employees or contractors accessing the Perceptyx network or other cloud-based networks or tools are required to use HTTPS/TLS 1.2+ at a minimum to protect data-in-transit.

iv. If employees or contractors are working in a public space, they must ensure their sight lines are blocked and must not have customer conversations or other confidential conversations. If someone is nearby, it must be assumed they can see and hear everything. Connecting directly to a public wireless network that does not employ, at minimum, WPA-2 or an equivalent wireless protocol, is prohibited.

v. While working at home, employees and applicable contractors must be mindful when visitors (e.g., maintenance personnel) are at their residences, as visitors could become privy to sensitive information left up on computer screens.

f. **System Access Security**

i. Perceptyx adheres to the principle of least privilege, specifying that team members will be given access to only the information and resources necessary to perform their job functions as determined by management or a designee. Requests for escalation of privileges or changes to privileges and access permissions are documented and require approval by an authorized manager. System access is revoked immediately upon termination or resignation.

1. **Account Audits**

a. Audits of access and privileges to sensitive Perceptyx applications, infrastructure, systems, and data are performed regularly and reviewed by authorized personnel.

g. **Password Security**

i. Unique accounts and passwords are required for all users. Passwords must be kept confidential and not shared with anyone. Where possible, all user and system accounts must invoke password complexity requirements specified in the Access Control and Termination Policy. All accounts must use unique passwords not shared with any other accounts.

ii. **Rotation Requirements**

1. If a password is suspected to be compromised, the password must be rotated immediately and the security team must be immediately notified.

iii. **Storing Passwords**

1. Passwords must only be stored using a Perceptyx approved password manager. Perceptyx does not hard code passwords or embed credentials in static code.

h. **Asset Security**

i. Perceptyx maintains a Configuration and Asset Management Policy designed to track and set configuration standards to protect Perceptyx devices, networks, systems, and data. In compliance with such policy, Perceptyx may provide team members laptops or other devices to perform their job duties effectively.

i. **Data Management**

i. Perceptyx stores and disposes of sensitive data, in a manner that; reasonably safeguards the confidentiality of the data; protects against the unauthorized use or disclosure of the data; and renders the data secure or appropriately destroyed. Data entered into Perceptyx applications must be validated where possible to ensure quality of information processed and to mitigate the impacts of web-based attacks on the systems.

ii. **Data Classification**

1. Perceptyx defines the handling and classification of data in the Data Classification Policy.

iii. **Data Retention and Disposal Policy**

1. The time periods for which Perceptyx must retain customer data depends on the purpose for which it is used. Perceptyx retains customer data as long as an account is active, as needed to provide services to the customer, or in accordance with the agreement(s) between Perceptyx and the customer. An exemption to this policy would include if Perceptyx is required by law to dispose of data earlier or keep data longer. Perceptyx may retain and use customer data to comply with legal obligations, resolve disputes, and enforce agreements.

j. **Change and Development Management**

i. **Vulnerability and Patch Management**
    1. Perceptyx uses a proactive vulnerability and patch management process that prioritizes and implements patches based on classification. Such classification may include whether the severity is security-related or based on other additional factors. Perceptyx schedules third party penetration tests and/or performs internal assessments at least annually.
    2. If you believe you have discovered a vulnerability, please email infosec@perceptyx.com and Perceptyx will aim to address the vulnerability, if confirmed, as soon as possible.
ii. **Environment Separation**
    1. As necessary, Perceptyx maintains requirements and controls for the separation of development and production environments.
iii. **Source Code**
    1. Perceptyx controlled directories or repositories containing source code are secured from unauthorized access.

k. **Logging and Monitoring**
    i. Perceptyx collects & monitors audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services, as well as IAM user and admin activities. Perceptyx manages logging solution(s) and/or SIEM tool(s) to collect event information of the aforementioned systems and activities. Perceptyx implements filters, parameters, and alarms to trigger alerts on logging events that deviate from established system and activity baselines. Logs are securely stored and archived for a minimum of 1 year to assist with potential forensic efforts.
    ii. Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. System and user activity logs may be utilized to assess the causes of incidents and problems. Perceptyx utilizes access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.
    iii. When events and alerts are generated from monitoring solutions and mechanisms, Perceptyx correlates those events and alerts across all sources to identify root causes and formally declare

incidents, as necessary, in accordance with the Security Incident Response Policy and Change Management Policy.

iv. Additionally, Perceptyx utilizes threat detection solution(s) to actively monitor and alert on network and application-based threats.

l. **Business Continuity and Disaster Recovery**
    i. Perceptyx maintains a plan for continuous business operations if facilities, infrastructure or systems fail. The plan is tested, reviewed and updated at least annually.
        1. **Backup Policy**
            a. Backups are performed according to appropriate backup schedules to ensure critical systems, records, and configurations can be recovered in the event of a disaster or media failure.

m. **Security Incident Response**
    i. Perceptyx maintains a plan that defines responsibilities, detection, and corrective actions during a security incident. The plan will be executed following the discovery of an incident such as system compromise, or unintended/unauthorized acquisition, access, use or release of non-public information. The plan is tested, reviewed and updated at least annually.
    ii. Perceptyx utilizes various monitoring and surveillance tools to detect security threats and incidents. Early detection and response can mitigate damages and minimize further risk to Perceptyx.
    iii. A message must be sent to infosec@perceptyx.com if you believe there may be a security incident or threat.

n. **Risk Management**
    i. Perceptyx requires a risk assessment to be performed at least annually. For risks identified during the process, Perceptyx must classify the risks and develop action plans to mitigate discovered risks.

o. **Vendor Management**
    i. Perceptyx requires a vendor security assessment before third party products or services are used confirming the provider can maintain appropriate security and privacy controls. The review may include gathering applicable compliance audits (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, etc.) or other security compliance evidence. Agreements will be updated and amended as necessary when business, laws, and regulatory requirements change.

p. **Privacy**
    i. Personal Data
        1. Perceptyx personnel must treat personal data with appropriate security and handling and accommodate data subject requests, as required by applicable laws and regulations. No unauthorized personnel must have access to personal data.

3. **Standards Alignment**
    a. This policy and associated procedures are designed to comply with the requirements of ISO 27001, including:
        i. A.5.1: Policies for Information Security
    b. SOC 2 Trust Service Criteria
        i. CC1.1
        ii. CC2.1
    c. CIS Controls v 8
        i. All 18 Controls
    d. NIST CSF
        i. Govern
        ii. Identify
        iii. Protect
        iv. Respond
        v. Recover
4. **Exceptions**
    a. Perceptyx business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other Perceptyx policy. If an exception is needed, Perceptyx management will determine an acceptable alternative approach.
5. **Enforcement**
    a. Any violation of this policy or any other Perceptyx policy or procedure may result in disciplinary action, up to and including termination of employment. Perceptyx reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Perceptyx does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.
    b. Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of Perceptyx as soon as possible.

c. The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

6. **Responsibility, Review, and Audit**
    a. Perceptyx reviews and updates the security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.