Information Security Overview

Perceptyx is committed to providing our customers with a secure and reliable SaaS platform. We understand the importance of protecting your data and maintaining the confidentiality, integrity, and availability of our services. To achieve this, we have implemented a comprehensive information security program based on industry-leading standards and best practices.

Key Components of Our Security Program

Our information security program comprises a combination of technical, policy, and people controls, working together to safeguard your information:

1. Information Security Management System (ISMS)

- We have established an ISMS based on the ISO 27001 standard. This framework provides a systematic approach to managing sensitive company information to ensure it remains secure.
- Our ISO 27001 certification demonstrates that our ISMS meets rigorous international standards for information security. An independent auditor has verified that our security controls are effectively implemented and maintained.
- The ISMS encompasses:
    - Risk management: We systematically assess information security risks and implement controls to mitigate them.
    - Policies and procedures: We have documented security policies and procedures that govern how information is accessed, used, and protected.
    - Continuous improvement: We regularly monitor, review, and improve our ISMS to adapt to evolving threats and business needs.

2. SOC 2 Type II Compliance

- We undergo regular SOC 2 Type II audits, which provide an independent assessment of our security controls.
- These reports validate the effectiveness of our controls over a period and confirm our commitment to:
    - Security: We protect customer data against unauthorized access, use, or disclosure.
    - Availability: We ensure our systems and services are available to customers as agreed.
    - Confidentiality: We protect sensitive information from unauthorized access and disclosure.
    - Processing Integrity: We ensure data is processed accurately, completely, and in a timely manner.
    - Privacy: As a data processor, we ensure personal information is handled in conformity with applicable data protection requirements.

3. Technical Controls

We employ a range of technical controls to secure our infrastructure and data. These controls are aligned with industry-leading practices, including those detailed in ISO 27002. Here's an overview of key areas:

- **Access Control:** We implement robust access control measures to ensure that only authorized individuals can access our systems and data. This includes:
    - Strong authentication mechanisms, such as multi-factor authentication, to verify user identities.

    - Authorization processes that enforce the principle of least privilege, granting users only the access necessary to perform their job functions.
    - Access logging and monitoring to track user activity and detect any unauthorized access attempts.
- **Network Security:** We maintain a secure network infrastructure with multiple layers of defense:
    - Firewalls to prevent unauthorized access to our networks.
    - Intrusion detection and prevention systems (IDS/IPS) to identify and block malicious network traffic.
    - Network segmentation to isolate critical systems and limit the impact of potential security breaches.
- **Data Protection**: We protect data both in transit and at rest:
    - Encryption of data in transit using secure protocols such as TLS to prevent eavesdropping.
    - Encryption of data at rest using strong encryption algorithms to protect data stored on our systems.
- **Vulnerability Management**: We proactively manage vulnerabilities in our systems and software:
    - Regular vulnerability scanning to identify potential weaknesses.
    - Timely patching and remediation of identified vulnerabilities.
    - Security configuration management to ensure that systems are configured securely.
- **Secure Development Practices:** We incorporate security into every stage of the software development lifecycle:
    - Secure coding guidelines to minimize vulnerabilities in our applications.
    - Regular security testing, including penetration testing and code reviews, to identify and address security flaws.
- **System Monitoring:** We continuously monitor our systems to detect and respond to security events:
    - Security information and event management (SIEM) systems to collect and analyze security logs.
    - Alerting mechanisms to notify security personnel of suspicious activity.
    - Incident response procedures to ensure a swift and effective response to any security incidents.

4. Policies and Procedures

Our security policies and procedures provide a framework for maintaining information security across the organization. These include:

- **Information security policy:** A high-level policy that outlines our commitment to information security and sets the direction for our security program.
- **Access control policy:** Defines rules for granting, managing, and revoking access to systems and data.
- **Privacy policy:** Outlines how we collect, use, and protect customer data, ensuring compliance with applicable privacy regulations.
- **Incident response plan:** Details the procedures for identifying, responding to, and recovering from security incidents, minimizing disruption and data loss.
- **Business continuity and disaster recovery policy:** Ensures that we can continue to operate our services and recover critical data in the event of disruptions or disasters.

5. People Controls

- We recognize that our employees play a vital role in maintaining our security posture. We implement the following people controls:

- Security awareness training: All employees undergo regular security awareness training to ensure they understand their security responsibilities and how to protect information.
- Background checks: We conduct background checks on employees as appropriate and in accordance with applicable laws.
- Confidentiality agreements: Employees are required to sign confidentiality agreements to protect sensitive information.
- Roles and responsibilities: Security roles and responsibilities are clearly defined and communicated to ensure accountability.

6. AI Governance

- We have a formal AI Governance framework based on the ISO 42001 standard. This framework provides a systematic approach to managing the processes and responsibilities necessary to ensure responsible AI development and usage within Perceptyx.
- As part of our overall AI Governance, we are actively pursuing ISO 42001 certification. Our initial audit is upcoming with an anticipated certification expected by December 2026.

By adhering to the ISO 27001 standard, undergoing SOC 2 Type II audits, and implementing ISO 42001 controls, we demonstrate our ongoing commitment to maintaining a robust security posture and protecting our customer's data. We continually invest in our security program to address evolving threats and ensure the confidentiality, integrity, and availability of our platform.