INFORMATION SECURITY POLICY

May 2026

TABLE OF CONTENTS

1. Purpose and Scope

At IperionX, information is a critical business asset. The purpose of this Information Security Policy is to establish a clear framework for protecting IperionX information systems and data from unauthorized access, misuse, loss, or disruption.

This policy is intended to ensure that information security practices support business operations, contractual obligations, risk management, and regulatory requirements while remaining understandable and actionable for all employees.

This policy applies to all employees, contractors, consultants, and third parties who access, use, store, process, or transmit IperionX information or use IperionX information systems.

IperionX executive management and the Nominating and Governance Committee of the Board of Directors have approved this Information Security Policy.

2. Responsibilities

Board and Executive Management

The Board of Directors, along with IperionX executive management, is responsible for overseeing compliance with this Information Security Policy and ensuring its implementation throughout the business.

Head of Information Technology

- Establish and maintain the company's information security program.
- Ensure information security policies align with business, contractual, and regulatory requirements.
- Provide oversight of security controls, risk management, and incident response activities.

Information Technology Department

- Implement and maintain technical and administrative security controls.
- Monitor systems for security threats, vulnerabilities, and unauthorized activity.
- Respond to, investigate, and remediate information security incidents.

Employees and Authorized Users

- Follow this policy and all related information security procedures.
- Protect company credentials, devices, and information.
- Promptly report suspicious activity or potential security incidents.

Suppliers

- Information Security practices are required of suppliers as noted in the IperionX Supplier Code of Conduct available on the IperionX website.

3. Information Security Policy Requirements

Policy Statement

IperionX is committed to protecting the confidentiality, integrity, and availability of company and customer information. Access to information is granted based on job responsibilities and business need. Security controls must not be bypassed, disabled, or circumvented.

Information Handling and Protection

IperionX information must be handled in accordance with its sensitivity and applicable contractual or regulatory requirements. Company information must not be stored in personal accounts, unapproved cloud services, or on unauthorized devices.

Access Control

Access to IperionX systems and information is approved by management and the Information Technology department and limited to the minimum necessary to perform assigned job duties. Access is reviewed periodically and removed when no longer required.

Security Awareness

All users are required to complete assigned information security awareness training and remain vigilant against threats such as phishing, social engineering, and malware.

Incident Reporting

Any suspected or confirmed information security incident must be reported immediately to the Information Technology department.

Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, and may also result in contractual or legal consequences where applicable.

4. Review and Continuous Improvement

Continuous Improvement

IperionX is committed to continuous improvement in its approach to information security and will adapt to changing circumstances and regulations or requirements.

Periodic Review

This policy will be reviewed periodically and updated as necessary to reflect changes in business operations, technology, or regulatory requirements.

Document History

Date	Revision#	Details
May 2026	0	Initial Issue