ASHTROM Group

Cybersecurity and Data Privacy Policy

Ashtrom Group

Ashtrom Group

is a leading construction and real estate company engaged in various activities, including construction, concessions, construction industries, development and marketing of residential projects, as well as the acquisition and management of income-generating properties

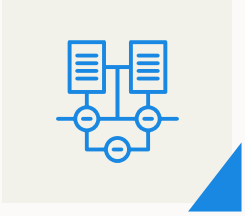
A significant portion of the Group's business operations is supported by its technological systems unit, which plays a central role in managing both sensitive business data and personal information. This information is safeguarded by the provisions of the Privacy Protection Law (1981) and the Privacy Protection (Information Security) Regulations (2017). Accordingly, the Group has established a Cybersecurity and Privacy Protection Policy that addresses the safeguarding of information in terms of confidentiality, integrity, and availability. The policy also outlines the Group's approach to mitigating various cyber threats, with the primary goal of ensuring the continued, uninterrupted operation of its technological systems.

The Group has set itself the goal of developing, implementing, and maintaining an appropriate level of logical and physical security to protect its information, assets, and technological infrastructure from unauthorized access, disruption, interruption, or shutdown. This commitment is essential to ensuring the continuity of the Group's business operations and maintaining compliance with all applicable legal and regulatory requirements related to information security and privacy.

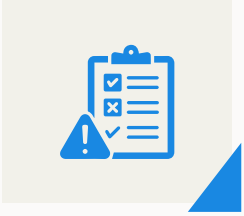
It should be noted that this policy is intended to serve as a comprehensive framework for safeguarding the Group's information and ensuring the protection of privacy. Nonetheless, it is important to emphasize that, despite the Group's ongoing efforts, it is not possible to provide an absolute guarantee against cyber incidents or privacy breaches. Cyber threats are dynamic and constantly evolving, and unforeseen events beyond the Group's control may occur. The Group implements reasonable and appropriate measures, as outlined in this policy, to mitigate risks; however, full adherence to the policy does not ensure complete immunity from cybersecurity or privacy-related incidents.

Applicability

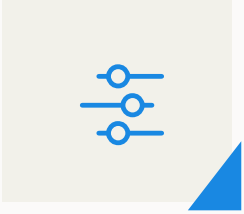
This policy applies to all business processes, systems, infrastructure, data, and information assets owned or managed by the Group. Its provisions are binding on all Group employees, as well as outsourced personnel, contractors, suppliers, and any other external parties who access, manage, or store the Group's sensitive information and/or are connected to its network.



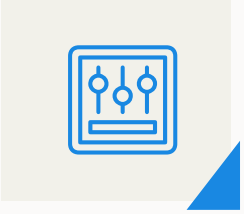
Mapping and classifying processes, systems, and information assets



Risk assessment



Conducting privacy impact surveys for business processes and information systems



Implementing controls and formulating a risk mitigation plan

the effectiveness of protection measures

Guidelines for Implementing the Policy

Cyber Risk Management and Privacy Protection

The Group manages cyber risks and privacy protection relevant to its business processes, systems, and information in an active, up-to-date, and ongoing manner, according to its best judgment and assessment and by the following stages:

Implementation of Cybersecurity and Privacy Protection Controls

The Group has defined and is actively working to implement managerial, operational, and technological controls aimed at reducing the risk of harm to the confidentiality, integrity, and/or availability of its information assets, information systems, business processes, and overall business operations.

Cybersecurity, Data Protection, and Privacy Protection

The Group has defined and is working to implement periodic controls designed to minimize cyber, data protection, and privacy risks associated with employee activities and the Group's ongoing operations. These controls are integrated throughout the employee lifecycle—from the recruitment stage (including screening, background checks, and credibility assessments) through to the termination of employment.

The Group has developed a comprehensive plan to raise employee awareness regarding cyber risks and privacy protection. This plan will be incorporated into the Group's annual work program and is designed to achieve the following objectives:

01 Enhancing knowledge of the cyber and privacy-related risks to which the Group is exposed

02 Promoting the necessary organizational awareness to identify and appropriately respond to cyber incidents relevant to employees' roles.

03 Implementing cybersecurity and privacy policies, including guidelines for the use of computing resources, email practices, password management, safe internet browsing, and the proper handling of personal and other sensitive information encountered during employment. These policy documents also define, among other things, the conditions under which employee and/or third-party information may be transferred, all by applicable legal requirements.

The Group places great importance on safeguarding the privacy of its employees, tenants, suppliers, and clients. Its privacy policy outlines the purposes for which personal information is collected, the types of data gathered, the permitted uses of such information, and the measures for managing and maintaining these databases.

The Group operates, among other things, by the principles of proportionality and purpose limitation when handling personal information received from third parties during engagements. In line with legal requirements, the Group has established cybersecurity and privacy protection policies and accordingly, manages and updates its databases, information security protocols, and agreements relating to confidentiality and privacy with suppliers, service providers, and partners. The Group also implements restrictions on advertising mailings and other measures, from time to time, at its discretion.

Systems, Communications, and Operations Security

Ashtrom Group takes reasonable and appropriate measures to protect its information, communications, and operational systems. These efforts are guided by principles established by the Group's cyber management and privacy protection authorities. The Group takes reasonable and appropriate measures to maintain the confidentiality of information, ensure the operational continuity of its information systems and business activities, and mitigate risks associated with its ongoing operations.

Logical Access Control

Ashtrom Group has established structured procedures for managing logical access control, in alignment with recognized cybersecurity and privacy protection principles, as part of its broader risk management and assessment framework. As part of the policy's implementation and supporting documents, the Group takes reasonable measures to manage, monitor, and protect digital identities. In addition, the Group periodically introduces processes for oversight, planning, and updating relevant policy documents, through control and validation mechanisms specifically established for this purpose.
The work procedures and documents accompanying this policy include defined standards for password security.

Information Security Surveys

Ashtrom Group carries out, as necessary and at its discretion, surveys on the subject of information security, including, among other things:

- Mapping and classifying processes, systems, and information assets
- Risk mapping and assessment
- Conducting privacy impact surveys for business processes and information systems
- Implementing controls and formulating a risk mitigation plan
- Measuring, ongoing monitoring, and identifying risks, as well as assessing the effectiveness of protection measures

Penetration Tests

The Ashtrom Group operates by a strategic policy for conducting information security assessments and penetration tests. These activities are intended to evaluate the presence and effectiveness of security controls implemented across various systems and processes.
The definition, management, and adaptation of these surveys are led by the Head of Cyber and Privacy Protection, with an emphasis on promoting compliance with regulatory requirements and recognized industry standards.
The plan for addressing, implementing, and monitoring survey findings will be updated and managed by the Head of Infrastructure and Information Security, in coordination with the Head of IT Systems Division. The plan will address the various aspects required for implementing corrective actions, as determined at their discretion, and will include timelines based on the level of risk. It will also outline the procedures for determining whether and how to address identified findings, taking into account business constraints and resource limitations.

Monitoring and Control of IT Systems

Ashtrom Group is working to implement advanced monitoring and control processes for managing and tracking cyber events across its various information systems. The objective is to support early detection of threats and incidents by analyzing information system data and tailoring responses to the organization's needs. This is achieved through monitoring systems that provide a real-time overview of the situation. The Group operates a managed service, staffed 24/7, which is responsible for overseeing monitoring activities and assisting in defining tailored responses to events, according to established policies.

Physical and Environmental Security

Ashtrom Group implements a range of reasonable and appropriate physical and environmental security measures to protect its information systems and the data stored within them from unauthorized access, physical damage, or disruption to ongoing operations. These controls are designed to ensure an adequate level of physical protection for the Group's critical assets. This includes the definition and implementation of physical security measures such as access mechanisms, access management procedures, and documentation protocols for controlling entry to sensitive areas.

Information Security and Cyber Incident Preparedness

01 Ashtrom Group develops, updates, and promotes the implementation of procedures and guidelines for managing information security and cyber incidents, aimed at ensuring an effective and controlled response to significant cyber and privacy-related events.

02 These procedures include defined response protocols and action plans for handling various cyber scenarios, outlining reporting formats and frequencies, as well as communication methods with relevant internal and external stakeholders.

03 The policy places a strong emphasis on incident management, structured around a series of defined stages, including:

- Detection
- Situation assessment
- Containment and mitigation attempts
- Advancement of recovery operations
- Restoration of normal operations
- Post-incident investigation

The Group conducts periodic exercises across various operational units to assess the effectiveness of its cyber incident preparedness. These exercises are designed to identify areas for improvement and implement corrective actions based on investigation findings and lessons learned. Key focus areas include backup systems, survivability, redundancy, disaster management, and disaster recovery processes, all within the framework of the Group's organizational cyber resilience strategy. The Group also leads the validation and ongoing updating of these plans in response to evolving needs, under the supervision and guidance of the Head of Cyber and Privacy Protection.

Promoting Information Security, Cyber Protection, and Privacy in Procurement and Contracting Processes

Ashtrom Group integrates principles of information security, cyber protection, and privacy protection into its key procurement and contracting processes with business partners, suppliers, and other external parties.

As part of this approach, the Group defines and enforces information security and privacy requirements within contractual agreements, including the implementation of various control measures. Any external party with access to sensitive information is required to sign confidentiality agreements as a precondition for engagement.

Policy Implementation

The implementation process includes regular internal communication, dedicated employee training on the policy and its associated procedures, and the execution of targeted activities aimed at preventing information security incidents in practice.

A central component of the policy and procedure implementation across all organizational levels is the involvement of authorized personnel, as defined in this document.

Corporate Governance Principles – Roles, Authority, and Responsibility

01 **The Board of Directors** – The Board of Directors is responsible for overseeing the Group's compliance with applicable privacy laws and regulations. This oversight includes:

- Ensuring the existence of an effective internal review, enforcement, and control plan
- Reviewing and discussing repository definition documents
- Reviewing the key principles of the Group's information security procedures
- Reviewing the results of risk assessments and penetration tests, including required corrective actions for identified deficiencies.
- Quarterly or annual (as appropriate) discussions of information security incidents that have occurred within the organization
- Review and discussion of the results of the mandatory biennial audit regarding compliance with applicable regulations

02 Information Systems Manager

The Information Systems Manager is responsible for overseeing the Group's information technology activities, including the management of technological and informational assets, as well as the business processes supported by these systems. This role includes responsibility for the implementation of the Group's cyber protection policy, privacy protection measures, and information security procedures, along with all associated guidelines, instructions, and documentation. In addition, the Information Systems Manager oversees the installation, operation, and maintenance of cybersecurity tools and technologies, including monitoring systems, backups, communications, IT infrastructure, and computing platforms across the Group. The role also includes ongoing responsibility for identifying, addressing, and mitigating information and cybersecurity exposures and vulnerabilities.

03 The Head of Cyber and Privacy Protection

Serves as the designated function in charge of privacy protection within the Group. Acting as a professional authority and central knowledge resource, this role is involved throughout the entire lifecycle of the Group's information processing activities and is tasked with ensuring compliance with the Privacy Protection Law and all applicable regulations.
The Head of Cyber and Privacy Protection is required to submit an annual report detailing the Group's privacy-related activities. Under the Group's full Cyber and Privacy Protection Policy, this individual may not assume any additional or subordinate roles that could compromise the integrity or independence of their responsibilities. Key responsibilities include conducting privacy impact assessments for the Group's business processes and information technologies, as well as overseeing the execution of privacy risk surveys.

04 Database Managers

Database Managers are responsible for ensuring compliance with legal requirements and privacy protection regulations concerning the databases under their management. They must adhere to the Group's policy documents and procedures and maintain consistent, ongoing, and effective oversight of the implementation of recommendations and corrective actions stemming from risk assessments and periodic penetration tests.

A detailed report on our activities in this area is available in the Group's ESG Report.

We welcome our stakeholders to share their feedback, suggestions, and ideas by contacting us at: privacy@ashtrom.co.il

Note: For convenience, this policy is written in the masculine form but is intended to refer equally to all genders.