Information Security, Cyber Protection and Privacy Policy – Ashtrom Group

ASHTROM Group
EXCELLENCE IN CONSTRUCTION

Ashtrom Group is a construction and real estate company that operates in various fields including contracting, industry, franchising, entrepreneurship, development and marketing of residential projects, property acquisition, and property management.

Most the Group's business activities are managed by the Technological Systems Department that is entrusted with the management of **sensitive business data** and **sensitive personal data** held by the Group and that is protected by virtue of the Privacy Protection Law 1981 and the Privacy Protection (Information Security) Regulations, 2017.

Accordingly, the Group has defined an Information Security, Cyber Protection and Privacy Policy, which refers to the protection of data regarding their **confidentiality, completeness, and availability**, as well as the concept of protection as it relates to various cyber threats, with the goal of protecting against the disruption of standard operations of the technological system on which the Group is established.

The Group has set out a goal of developing, implementing, and maintaining an acceptable level of logical and physical security to protect the data, assets, and technological infrastructure in its possession against unauthorized access, disruption, interference or shutdown, all in order to ensure the proper continuity of its business activities and compliance with the relevant legal provisions applicable to it in connection with this topic.

Application of the Policy

The provisions of this policy apply to all business processes, systems, infrastructure, data, and information assets that belong to the Group, and are binding for all the Group's employees as well as outsourced employees, contractors, suppliers, and other external parties who have a user profile on the Group's network and/or who access/manage/store sensitive information belonging to Group.

Guidelines for Policy Implementation

Information Security and Cyber Risk Management

The Group manages the information security and cyber risks relevant to its business processes, systems, and data in an active, timely, and on-going manner, according to the following steps:

- Mapping and classification of processes, systems, and data assets
- Risk assessment
- Implementing controls and formulation of a risk reduction plan
- Ongoing measurement and identification of risks and evaluation of protective measures

Implementation of Controls for Information Security and Privacy

The Group has defined and implements managerial, operational, and technological controls, with the aim of reducing the risk of damage to the confidentiality, completeness and/or availability of its data assets, information systems, business processes, and its standard business activity.

Information Security and Privacy

- The Group has defined and implements periodic controls to minimize information security risks arising from the activities of its employees. These controls are implemented throughout all the stages an employee's engagement with the Group, beginning during the recruitment process (screening, background checks, and reliability checks) and through to termination of employment.
- The Group formulated a plan to raise employee awareness on information security and cyber risks, which will be integrated into the annual work plan, and will be adapted to the various employee groups, including outsourced employees and field agents, and which will work to achieve the following goals:
  - Increasing knowledge regarding information security and cyber risks to which the Group is exposed;

- Raising organizational awareness to the requisite level for identifying and responding to cyber incidents arising from the nature of the job and requests from employees to approve of the Group's Privacy Policy;
- Implementation of information security and cyber protection procedures and individual training on the relevant procedures for the employee groups, including the use of computers, email, password management, as well as management of personal and other data that the employee comes into contact with in the course of their work for the Group. The procedures regulate the conditions for transferring information about employees and/or third parties, all according to the directives provided by law.

- The Group considers it essential to protect the privacy of its employees. Our Privacy Policy includes references to the purposes for which data is collected from the employees, the types of data collected, the uses that can be made of this data, and the ways in which the Group handles and maintains this database. The information collected and managed by the Group has many uses that benefit both it and the employees, which predominately include:
  - Management of the Group's human resources and the services provided to employees.
  - Protection against leakage of trade secrets, protection of Ashtrom's intellectual property, copyrights, and interests.
  - Managing the Group's business activities in accordance with defined policy documents and procedures.

In addition, the Group acts according to these principles regarding maintaining the privacy of the data received from other third parties during the engagement period between parties. In accordance with the requirements of the law, we have formulated privacy and information security procedures and accordingly, perform registration and updating of databases, apply information security agreements with suppliers and in various engagement agreements, implement restrictions for mailing advertisements, and more. All this is performed in addition to the activities previously described regarding the protection of employee privacy and extensive training on the topic.

Security of Systems, Communications and Operations

The Group works to implement controls on the security of systems, communications, and operations, with the goal of protecting the completeness and reliability of the data, maintaining the functional continuity and intactness of information systems, the supporting infrastructure and business activity, controlling the spread of attacks and ensuring the ability to restore systems and recover while minimizing the extent of damage caused.

Logical Access Control

The Group has defined procedures for the various processes in lifecycle management of users, including creation of a user account, managing, and changing privileges and authorizations, locking an account, and more. The procedures include references to the method of execution, provision of means of identification, parties responsible for implementation, agreed upon approving parties, periodic review processes and additional controls.

Access passwords will comply with accepted security standards. The Group has defined a password policy that includes a minimum number of characters, required complexity, frequency of changing the password and rules for using and saving the password.

Information Security Studies

The Group formulated a plan to carry out studies and penetration tests to evaluate the existence and effectiveness of the process and system protection controls, while covering all levels of security, including at the infrastructural, application, logical and environmental levels.

The manager of the topic will update and manage a plan for handling and monitoring the findings of the studies, which will include reference to the factors responsible for implementing the corrections, timelines according to the level of exposure, and the method of handling and/or not handling the findings.

Monitoring and Control of Information Systems

The Group implements notifications and controls to monitor cyber incidents in the information systems.

Physical and Environmental Security

The Group works to implement environmental security controls to prevent unauthorized access, damage and/or interference with the data and systems.

According to this framework, protective measures and controls were defined with reference to required physical access controls according to the sensitivity of areas and regarding the management of security processes for maintaining and eliminating equipment and documentation.

Preparedness for Information Security and Cyber Security Events

- The Group has defined procedures and instructions (playbooks) for managing information security and cyber security incidents, which specify the manner of response and methods of action for managing various cyber scenarios, the format and frequency of reporting incidents and the manner of contacting internal and external parties, referring to each of the stages of incident management:
    - Identification
    - Assessment
    - Containment and Eradication
    - Recovery
    - Return to Routine
- The Group conducts periodic drills regarding all the relevant configurations, with the goal of testing the effectiveness of the preparation plan, implementing corrections, and identifying areas for improvement in accordance with the findings of the drills and the lessons learned. Additionally, the Group updates these plans periodically.

Promoting Information Security and Privacy Across Our Value Chain

We encourage the implementation of the guiding principles detailed in this policy across our value chain and communicate the importance of the issue to our business partners, suppliers, and other parties with whom we do business. We consider this to be fair and honest business conduct that secures all parties involved in the engagement, along with being necessary for compliance with the existing regulations in the field. We agree upon the matter at the point of engagement.

<u>Information security controls regarding outsourcing and supplier management:</u>

The Group defined a procedure that regulates aspects of information security and privacy as they relate to engagements with external parties. As part of the procedure, the controls relevant to the process of engaging with an external party were defined in relation to the outsourcing risks and supply chain security, as well as the required involvement of the field manager in the process.

Any engagement process with an external party, including the purchase of external IT services and among them the use of cloud-based services, will be conducted while integrating information security requirements and aspects.

In addition, the Group defined a procedure for determining the conditions and manner of providing remote maintenance services by an external service provider.

Any external party that, as part of its engagement with the Group, may be exposed to sensitive information, is required to sign a confidentiality agreement and adhere to additional security restrictions that will be determined according to the nature of the service it provides and the way it accesses/receives the information. The abovementioned will be a precondition for engaging with that party.

Implementation of the Policy

This policy constitutes a framework for a variety of processes carried out by the Group to ensure full implementation and integration of the policy, beginning with internal organizational communication, trainings on the policy and related procedures, as well as conducting dedicated activities to prevent incidents in practice.

Corporate Governance for Policy Implementation – Roles and Responsibilities

- **Cyber and Privacy Protection Manager**: The Group has appointed a designated manager who is responsible for overseeing cyber security and privacy protection, and who will determine and update work procedures, work to raise employee awareness and implement the Group's principles and policies in this area.
- **Information Security and Cyber Risk Management Steering Committee**: The Group established a dedicated steering committee that meets every six months and is responsible for oversight and policy instruction in all aspects related to the proper management of the topic of information security, in accordance with risks, policies, external and internal guidelines and the Group's requirements.
- **Ashtrom Group Management**: Committed to the supervision of the information security management framework and its implementation, Ashtrom Group's management conducts an annual discussion on information security risk management, reviewing the annual information security and cyber protection work plan.

Publication and Communication of the Policy

Ashtrom Group's Information Security, Cyber Protection and Privacy Policy is accessible to all stakeholders on the Group's website.

The Group publishes information on its relevant activities in our ESG report.

We invite our stakeholders to submit feedback, suggestions, and thoughts on the topic to: privacy@ashtrom.co.il