Heimstaden BOSTAD

GROUP POLICY
Cyber Security

Policy owner: *Chief Technology Officer*

Approver: *CEO*

1. Policy Owner Purpose and Mandate

The policy's main objective is to ensure that Heimstaden Bostad (HSTB) has a high-quality and aligned Cyber Security Policy throughout the organization. The security policy defines what to protect and what to expect of the system users. It provides a basis for security planning when designing new applications or expand the current network and services. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords.

The Chief Technology Officer (CTO) is given the mandate to administer the Cyber Security Policy implementation throughout HSTB with an aim to have an updated framework for Cyber Security that support HSTB in achieving and securing its ambitions and goals.

2. Requirements from Group

1. CTO shall ensure the implementation of the Cyber Security Policy and framework and provide support and guidance throughout the organization, with regards to IT Security activities in the country and from HSTB.
2. Each country shall utilize HSTB's Cyber Security Policy, it's framework and tools, as further specified in HSTB Cyber Security Manual.
3. CTO and each country shall continuously identify, assess, and respond to Cyber Security issues and threats that can affect the company or its framework conditions. In addition, continuously identify, assess, and execute on opportunities to increase the Cyber Security level of the company.
4. CTO and each country shall ensure that a high level of Cyber Security is implemented across the organization and between units which will increase employees' knowledge about Cyber Security and how to protect the Cyber assets.

3. Reporting

- Each country shall report its top Cyber Security implementations, actions and issues to CTO quarterly i.e., as part of the Quarterly Business Review.
- CTO shall report highlighted topics from the countries in addition to the most important tasks and processes in Group function and share reports with management and board. CTO has meetings with all countries quarterly.
- Significant Cyber Security related risks at country level shall be reported by Country Manager to Country Risk Manager and CTO and other relevant Group function without undue delay.

4. Reference Documents

- Code of Conduct
- Cyber Security Manual