|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Entity:**  BPTP INTERNATIONAL TRADE CENTRE LIMITED | **Section:**  GOVERNANCE POLICY | | **Version:** V2 | | **Effective Date:** 01.07.2023 |
| **Subject:** CYBERSECURITY POLICY | | | | | |
| **Policy Owner:**  C-HRO | | **Review Date:**  01.07.2024 | | **Pages:**  1 | |

**Cybersecurity Policy**

**APPLICABILITY:** It applies to all projects, including both new construction and existing buildings at BPTP INTERNATIONAL TRADE CENTRE LIMITED.

**PURPOSE:** The purpose of a cybersecurity policy for BPTP Limited is to protect an organization's digital assets, sensitive information, and ensure the integrity of its operations. It articulates the organization's commitment to maintaining the confidentiality, integrity, and availability of information and systems.

**POLICY OUTLINE:** This policy outlines the principles and guidelines for ensuring the confidentiality, integrity, and availability of our information and information systems. It also aims to create a secure and resilient digital environment, safeguarding both our assets and the trust of our clients and stakeholders.

To support this policy, BPTP will:

* Committed to complying with all relevant laws and regulations concerning cybersecurity and data protection.
* Establish a designated individual or team responsible for overseeing cybersecurity initiatives.
* Implement strong access controls, including user authentication and authorization mechanisms.
* Enforce the principle of least privilege to limit access to necessary resources.
* Deploy firewalls and intrusion detection/prevention systems to secure our network infrastructure.
* Regularly update and patch network devices and software.
* Secure end-user devices with antivirus software, encryption, and regular software updates.
* Implement a mobile device management (MDM) solution for company-owned mobile devices.
* Define guidelines for handling, storing, and transmitting sensitive data.
* Encrypt sensitive information both in transit and at rest.
* Develop and maintain an incident response plan that outlines steps to be taken in case of a cybersecurity incident.
* Conduct regular cybersecurity awareness training for all employees to educate them about potential threats and best practices.
* Secure physical access to data centres, server rooms, and other critical infrastructure.
* Conduct regular cybersecurity audits and assessments to identify vulnerabilities and ensure the effectiveness of security controls.

**RESPONSIBILITY:** All individuals associated with BPTP namely, contractors, employees, suppliers, third-party vendors, consultants and other stakeholders who have access to systems, data and network must comply with the rules and regulations of the BPTP.

**AMENDMENTS:** This policy is subject to any changes in the applicable laws, rules and regulations by the management.