Adventz Securities Enterprises Limited

Cyber Security Policy

Cyber crimes are becoming more and more common across the world, making cyber security of the top priorities for everyone. Consequently, there has been a rapid increase in various cyber laws. In order to protect our company from numerous cyber-crimes, we need to have a clear and organized cyber security policy.

This cyber security policy is for our employees, vendors and partners to refer to when they need advice and guidelines related to cyber law and cyber crime. This cyber security policy will strive to protect company's data and technology infrastructure.

This policy applies to all of company's employees, contractors, volunteers, vendors and anyone else who may have any type of access to company systems, software and hardware.

- Logging in to any of company's accounts for personal devices such as mobile phones, tablets or laptops, can put our company's data at risk. Accessing any company's data from personal devices is not permitted. If so is inevitable, employees are obligated to keep their devices in a safe place, not exposed to anyone else and such incident should immediately be reported to the Chief Information Officer.

- Physical security practices to be followed by employees in relation to their workstations:
  1) Keep electronic devices password secured and protected
  2) Install security updates on a regular basis
  3) Upgrade antivirus software on a regular basis
  4) Don't ever leave your devices unprotected and exposed
  5) Lock your computers when leaving the desk

- **Email Security**

  Emails can carry spams or malevolent software (for example worms, bugs etc.). In order to avoid virus infection or data theft, our policy is always to inform employees to:

  1) Abstain from opening attachments or clicking any links in the situations when its content is not well explained
  2) Make sure to always check email addresses and names of senders.
  3) Search for inconsistencies
  4) Be careful with clickbait titles (for example offering prizes, advice, etc.)
  5) In case that an employee is not sure if the email received, or any type of data is safe, they can always contact our IT specialist.

- **Transferring Data**

  Data transfer is one of the most common ways cybercrimes happen. Follow these best practices when transferring data:

  1) Avoid transferring personal data such as customer and employee confidential data

2) Adhere to personal data protection law
3) Data can only be shared over company's network
4) Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies

- **Internet Usage**

Following activities are prohibited with regard to use of Internet within the organisation

- Downloading illegal software on the company's equipment.
- Downloading softwares without approval of the Chief Information Officer.
- Accessing suspicious websites.
- Accessing social networking websites.
- Uploading Company's information assets on any website except to fulfil the regulatory requirements based on the job profile.
- Accessing internet for personal use.

- **Additional Measures**

- Report stolen or damaged equipment as soon as possible.
- Report a perceived threat or possible security weakness in company systems.

- **Working Remotely**

Even when working remotely, all the cybersecurity policies and procedures must be followed.

- **Disciplinary Action**

When best practices and company's policy are not followed, disciplinary actions take place which may include

1) In case of breaches that are intentional or repeated, and are harmful to our company, company may take serious actions including termination
2) Depending on how serious the breach is, there will be 3 warnings
3) Each incident will be evaluated
4) Each case and incidence will be assessed on a case-by-case basis
5) Everyone who disregards company's policies will face progressive disciplinary action.

- **Review of the Policy**

The Company is required to review the above policy in every two years based on its own experience, business need and RBI guidelines in this regard.