Adventz Securities Enterprises Limited

Information Asset Classification Policy

Purpose

Many different kinds of information reside on company's network and the systems thereupon. Some of this information is public and would not be harmful to the Company if disclosed or compromised whereas other information is very confidential and would be extremely damaging if disclosed or compromised. Most information exists in between these two extremes.

Statement of Policy

The Company adopts and supports policies, procedures and guidelines that ensure the proper classification and protection of Company information assets. Company information is classified as one of the following types:

1. **Public:**
   This information is suitable for public dissemination. Examples include public web pages, course listings, press releases, marketing material, etc.

2. **Internal:**
   This information is available to all employees within the Company. Access to this information is restricted to use by employees only for the conduct of company business. Examples include strategic plans, organisation financial documents, budgets, recruitment plans, network diagrams, etc.

3. **Restricted:**
   Restricted information includes information that departments may decide to share with other departments outside their administrative purview for the purpose of collaboration. Examples include data created by the department, research data and project data, financial data etc. Loss of this information could cause harm to the Company's image or reputation, but would not necessarily violate existing laws or regulations.

4. **Confidential:**
   Confidential information is typically non-public information about people. Examples include legal records, financial account information etc. Data owner grants access to confidential information to data users, however data users are not allowed to disseminate this confidential information outside their administrative purview. Unauthorized release or loss of confidential information could reasonably be expected to cause legal and/ or financial consequences to the Company.

All information must be classified into confidentiality levels

The asset owner is responsible for classifying the information – and this is usually done based on the results of the risk assessment: the higher the value of information (the higher the consequence of breaching the confidentiality), the higher the classification level should be.

Classification criteria

The level of confidentiality is determined based on the following criteria

- Value of Information
- Sensitivity and Criticality of Information
- Legal and contractual Obligations

Information classified as “Restricted” and “Confidential” must be accompanied by a list of Authorised Persons. Access to such Information can be granted to other users only with the prior permission of the Data Owner and the Chief Information Officer.

Reclassification

Assets owners must review the confidentiality level pf their information assets every two years.

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.