FANO 有光科技 Labs

DATA SECURITY POLICY

Policy Statement

This document defines the data security policy of Fano Labs. To improve our operating efficiency, we are going to be more transparent with our employees on confidential or secret data such as financial or operating status of our company, and our source codes and datasets. These data are important assets of Fano Labs, which, if leaked, will have traumental consequence on our company. As such, while we will rely on our employees to be disciplined towards protecting our data, we will protect our rights by taking legal actions against any current or former employees who leaked our confidential or secret data for whatever purpose.

Objectives

The goal of this policy is to inform all employees at Fano Labs of the rules and procedures relating to data security compliance.

Audience

This policy applies to all employees, management, contractors, vendors, business partners and any other parties who have access to our data.

Data Classifications

We classify our data into the following three categories:

- Public
- Restricted
- Confidential
- Secret

Public

9.4.1.1 This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Public data include, but are not limited to:

- marketing materials
- product white papers, brochures

9.4.1.2 Employees may send or communicate a public piece of data with anyone inside or outside of the company.

Restricted

9.4.2.1 This is defined as internal information that is to be kept within the company. Access to this data is limited to internal staff and cannot be distributed outside of the workplace. Restricted data include, but are not limited to:

- company policies and procedures
- all internal communications
- all information stored in one drive, confluence, Jira and other storages provided by the company

All information not otherwise classified will be assumed to be restricted.

All employees must not disclose confidential data to anyone who is not a current employee. In no circumstance an employee shall share restricted data with any third parties unless proper confidentiality agreements are in place with such party.

Confidential

9.4.3.1 This is defined as sensitive information that is to be accessible within specific departments or personnel. Access to this data may be limited to specific departments or personnel and cannot be distributed outside of the workplace. Confidential data include, but are not limited to:

- payroll data
- accounting data

Employees may only share confidential data within the department or named distribution list and password protection should be applied if employee is sending the confidential dat via email. In no circumstance an employee shall share confidential data with any third parties unless proper confidentiality agreements are in place with such party.

Disposal of confidential data should be conducted in a secure manner such as shredding.

Secret

This is defined as sensitive data which, if leaked, would be harmful to Fano Labs, its employees, contractors and other parties as applicable. Access to secret data is restricted.

Secret data include but are not limited to:

- Source codes
- Customer data (voice recordings, text data etc.)
- Datasets, whether or not developed by Fano Labs or publicly available

- Financial information such as audit reports, legal documentation, business strategy details
- Information about the operating status of Fano Labs, either communicated in writing or orally (such as through a All-hands meeting)

All employees must not share secret data with anyone who is not a current employee. Employee should only share secret data on a **"need to know"** basis and password should be applied if employee is sending the secret data via email.. In no circumstance an employee shall share secret data with any third parties unless proper confidentiality agreements are in place with such party.

Disposal of confidential data should be conducted in a secure manner such as shredding.

Responsibilities

All employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy. The team head or department head is responsible for ensuring that their direct reports understand the scope and implications of this policy.

The human resource team must also ensure that each employee has signed a copy of this policy.

The ownership of this policy falls to the human resources team. For any questions about this policy, or to report misuse of corporate or personal data, please contact him at hr@fano.ai.

Security Measures in Place

The Infrastructure team will use accepted technologies to enforce and ensure data security, which include but not limited to:

- Access controls
- Strong passwords
- System monitoring system

The above security measure may change from time to time without further notice.

Regular Review

The human resources team is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.

The infra team is responsible for maintaining adequate security measures. These security measures will be reviewed annually or as circumstances arise.

Enforcement

Any employees found to be in violation of this policy by either unintentionally or maliciously stealing, using or otherwise compromising confidential or secret data may be subject to disciplinary action.

The company has reserved not less than US$500,000 to protect our data security. In case any current or former employee steals our source code or any other secret or confidential data, we will use this budget to ensure that our interests are protected, and that employee will receive the desired penalty.