Information Security Violations

Types of Security Violations

Information security is critical to the operations of Acuiti Labs. Violations of information security policies can have severe consequences. The following are types of security violations:

- **Unauthorized Access:** Accessing systems, data, or areas without proper authorization.
- **Data Breach:** Unauthorized disclosure or leakage of confidential information.
- **Use of Unauthorized Software:** Installing or using software not approved by the company.
- **Physical Security Breach:** Unauthorized entry into secured areas or improper handling of access cards.
- **Sharing of Credentials:** Sharing passwords, tokens, or access cards with unauthorized individuals.
- **Inappropriate Use of Company Resources:** Using company systems to access, store, or transmit inappropriate content.
- **Violation of Regulatory Requirements:** Non-compliance with data protection laws, such as GDPR or other regional regulations.
- **Negligence:** Leaving systems unattended or failing to secure sensitive information properly.

Reporting and Handling Security Violations

Prompt reporting and effective handling of security violations are essential to mitigate risks and ensure compliance.

- **Reporting Channels:** Employees should report any suspected or actual security violations immediately using designated channels, such as **isms@acuiticonsultants.com**, or through their reporting manager or HR.

- **Confidential Reporting:** Employees can report violations anonymously if they prefer, and their identity will be protected to the extent possible.
- **Initial Assessment:** Upon receiving a report, the Chief Information Security Officer (CISO) or a designated investigator will conduct an initial assessment to determine the severity and scope of the violation.
- **Investigation:** A thorough investigation will be conducted, including gathering evidence, interviewing involved parties, and reviewing relevant documents and logs.
- **Documentation:** All findings and actions taken during the investigation will be documented in detail.

Disciplinary Actions for Security Violations

Appropriate disciplinary actions will be taken based on the severity of the security violation. These actions aim to address the issue and prevent future occurrences.

- **Verbal Warning:** For minor, first-time violations that did not cause significant harm.
- **Written Warning:** For repeated minor violations or more serious breaches that pose a moderate risk to the company.
- **Suspension:** For serious violations that compromise sensitive information or disrupt operations. The employee may be suspended while the investigation is ongoing.
- **Termination:** For severe violations, such as deliberate data breaches, significant regulatory non-compliance, or repeated serious offenses.
- **Other Actions:** Depending on the nature and impact of the violation, additional actions may include:
    - **Mandatory Training:** Requiring the employee to undergo training on information security policies and practices.
    - **Access Revocation:** Restricting or revoking access to certain systems or data.
    - **Restitution:** Requiring the employee to compensate for any losses or damages caused.

Each disciplinary action will be documented, and the employee will be informed of the decision and the reasons behind it. The company will ensure that the disciplinary process is fair, consistent, and compliant with applicable laws and regulations.