Information Security and Confidentiality Policy

1. Information Security Policy

- An Information Security Policy will be established, maintained, and reviewed annually to ensure effectiveness and compliance with applicable law and regulation.
- This policy applies to all employees, contractors, and temporary staff.
- The policy will be easily accessible and communicated regularly, including during onboarding and upon revisions.

2. Non-Disclosure and Confidentiality

- Employees must respect the confidentiality of company and customer information during and after their employment.
- Confidential information must not leave the company premises or systems without prior authorization.
- Compliance with International Traffic in Arms Regulations (ITAR) is mandatory. Employees must ensure that access to ITAR-controlled information and materials is restricted to U.S. persons only, unless specifically authorized under a valid export license or other applicable ITAR exemption. All ITAR violations must be reported immediately to the designated compliance officer.

3. IT Equipment Usage

- Employees must adhere to the company's IT equipment usage rules, including:
    - Prohibition of unauthorized personal device use for business purposes. Personal devices are allowed for Office 365 if Microsoft's Mobile Device Security has been installed.
    - Mandatory reporting of lost or stolen devices immediately.
    - Returning IT equipment and access rights upon termination of employment.

4. Compliance and Training

- All employees are required to complete annual training on information security and confidentiality policies.
- Regular updates on laws, regulations, and company standards will be communicated to staff.
- Employees in sensitive roles (e.g., R&D, procurement) may receive additional, specialized training.

5. Handling of Personal and Confidential Information

- Personal information will only be collected, used, and shared in accordance with applicable laws.
- Employees must adhere to the procedures for storing, accessing, and disposing of sensitive data.
- Breaches or potential breaches must be reported immediately to the IT Manager or CFO.
- Access to personal information shall be limited to those who need access for their job duties, e.g. payroll, and Human Resources.

6. Access Control

- Access to sensitive areas and systems will be restricted to authorized personnel only.
- Entry and exit to restricted areas must be logged and monitored.
- Access rights will be reviewed annually and adjusted as necessary.

7. Cybersecurity Measures

- Anti-virus and endpoint protection software must be installed and regularly updated on all devices.
- Employees are prohibited from installing unauthorized software. All software installations must receive prior approval from the IT department.
- Multi-factor authentication is required for systems handling sensitive information.
- The following restrictions on the use of websites and web applications are in place and communicated to all employees:
    - Do not post company information on social media without prior permission.
    - Do not upload business data to web services without explicit authorization.
    - These restrictions apply to all executives, employees, temporary employees, and seconded employees.

8. Incident Response

- Procedures for responding to information security incidents, including malware attacks and data breaches, are documented in the Incident Response Guide.
- All incidents must be reported immediately, and response procedures will be reviewed annually.

9. Remote Work Policy

- Employees working remotely must use company-approved devices and secure connections.
- Confidential information must not be downloaded or stored on personal devices.

- Compliance with remote work policies will be verified annually.

10. Physical Security

- Server rooms and other sensitive areas must remain locked with access limited to authorized personnel.
- Logs of entry and exit to these areas will be maintained for six months.
- Measures to prevent unauthorized access, such as surveillance and identity verification, will be in place.

11. Disposal of Equipment and Data

- Data stored on devices must be irreversibly deleted before disposal or at the end of a lease.
- Records of data disposal will be maintained for compliance purposes.

12. Monitoring and Review

- The effectiveness of this policy will be reviewed annually or after any significant incidents.
- Updates and revisions will be communicated promptly to all employees.

This policy ensures a baseline framework for maintaining the confidentiality, integrity, and security of company and client information while adhering to applicable laws and industry best practices.