Data Security Policy

This Data Security Policy outlines behaviors expected from employees and business partners when dealing with Company data as well as the measures implemented by the Company to prevent sensitive data breaches.

Shared information is a powerful tool, and loss or misuse can cause reputational damage and can be costly, if not illegal. This Data Security Policy intends to protect the information assets of [COMPANY NAME].

Sensitive information must therefore be protected from unauthorized disclosure, modification, access, use, destruction or delay in service. Sensitive information includes but is not limited to:

- Unpublished financial information (budget, investments, etc.)
- Patents, formulas or new technologies used
- Private data of employees/customers/partners/vendors[1]
- Customers and contracts list (existing and prospective)

Each user has a duty and responsibility to comply with the information protection policies and procedures described in this document.

1. Purpose

The purpose of this Policy is to establish standards to safeguard data belonging to [COMPANY NAME] that is owned and/or operated by [COMPANY NAME] or equipment that is accessed by our internal systems.

This Policy particularly aims at:

- Protecting information from unauthorized access or misuse - including unauthorized electronic access (cybersecurity)
- Ensuring the confidentiality of information
- Maintaining the integrity of information
- Maintaining the availability of information systems and information for service delivery
- Complying with regulatory, contractual and legal requirements
- Maintaining physical, logical, environmental and communications security
- Disposing of information in an appropriate and secure manner when it is no longer in use

[1] *See our Data Privacy Policy*

2. Scope

This Data Security Policy applies to all Company's employees, contractors, volunteers, and anyone who has permanent or temporary access to the company's information (third party data, personal data and other company data), systems and hardware.

This Policy applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. It also applies to informal information sharing, i.e., other than by physical means (e.g., a conversation between individuals).

Information that is classified as Public is not subject to this Policy. Other data can be excluded from the Policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.

3. Authorized users

User identity
All users of **[COMPANY NAME]**'s information systems must be formally authorized by [specify department or role]. Authorized users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person.
Authorized users shall take all necessary precautions to protect the **[COMPANY NAME]** information in their personal possession.

Confidential, personal or private information must not be copied or transported without consideration of:

- the permission of the owner of the information;
- the risks associated with loss or falling into the wrong hands
- how the information will be secured during transport to its destination.
- other

Facilities & Workstations Access
[COMPANY NAME] will implement physical and technical safeguards for all facilities and workstations that access material and electronic confidential information to restrict access to authorized users.

Appropriate measures include:
- Monitoring offices 24x7 by an alarm system with video-surveillance capabilities
- Accessing facilities will be controlled with the use of card readers and locked doors
- Enabling physical access to **[COMPANY NAME]** facilities to individuals only identified with authorization credentials (badges, identity cards, etc.)
- Escorting visitors and monitoring their activities at all times
- Restricting physical access to workstations to only authorized personnel
- Securing workstations (screen lock or logout) prior to leaving the area to prevent unauthorized access

- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
- Storing all confidential information on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets
- Installing privacy screen filters or other physical barriers to public viewing
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates
- Other

4. Acceptable Use Policy (AUP)

While **[COMPANY NAME]**'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of **[COMPANY NAME]**.

Any information that users consider sensitive or vulnerable should be encrypted. For security and network maintenance purposes, authorized individuals within **[COMPANY NAME]** may monitor equipment, systems and network traffic at any time.

- User accounts on the company's computer systems must only be used for the company's business and must not be used for personal activities during working hours.

- During breaks or mealtimes, limited personal use is permitted, but use must be legal, honest and decent while considering the rights and sensitivities of others.

- Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

- Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager.

- Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Unauthorized use of the system may constitute a violation of the law, theft, and may be punishable by law. Therefore, unauthorized use of the company's computer system and facilities may constitute grounds for civil or criminal prosecution.

The fundamental element of this Data Security Policy is the control of access to critical information resources that require protection against unauthorized disclosure or modification.

Access control refers to the permissions assigned to persons or systems that are authorized to access specific resources. Access controls exist at different layers of the system, including the network. Access control is implemented by username/password/other. At the application and database level, other access control methods can be implemented to further restrict access.

Finally, application and database systems can limit the number of applications and databases available to users based on their job requirements.

5. Normal User Identification

All users must have a unique username and password to access the systems. The user's password must remain confidential and under no circumstances should it be shared with management and supervisory staff and/or any other collaborator.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed regularly, at least every **[NUMBER]** months.

All users at **[COMPANY NAME]** should be aware of how to select strong passwords. Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
    1. Lower case characters
    2. Upper case characters
    3. Numbers
    4. Punctuation
    5. "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

- Contain at least eight to fifteen alphanumeric characters
- User accounts will be frozen after **[NUMBER]** failed login attempts
- Login IDs and passwords will be suspended after **[NUMBER]** of days without use
- The password is NOT a word found in a dictionary (English or foreign)
- The password is not a common usage word such as:
    1. Computer terms and names, commands, sites, companies, hardware, software
    2. Passwords should NEVER be "Password1" or any derivation
    3. The words "**[COMPANY NAME]**", "**[City]**", or any derivation
    4. Names of family, pets, friends, co-workers, etc.
    5. Birthdays and other personal information such as addresses and phone numbers
    6. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    7. Any of the above spelled backwards
    8. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Below are some important points to remember:

- Users shall not share their passwords with anyone, including administrative assistants or secretaries, neither written nor spoken.

- Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

- Users will not be allowed to login as a System Administrator. Users who need this level of access must contact [department or position].

- Employee Login IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the company office.

- Employees who forget their password must contact [specify department or position] to get a new password assigned to their account.

- Employees will be responsible for all transactions occurring during Login sessions initiated by use of the employee's password and ID.

- Employees shall not login to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

6. Confidentiality of Information

Any information or documents that are not to be made public are designated as "Confidential Information". This information is invaluable to the company and therefore, all employees or business partners who, in the course of their duties, handle this type of information are expected to behave as follows:

- All confidential documents should be stored in locked file cabinets or rooms accessible only to those who have a business "need-to-know."
- All electronic confidential information should be protected via firewalls, encryption and passwords
- Employees should clear their desks of any confidential information before going home at the end of the day
- Employees should refrain from leaving confidential information visible on their computer monitors when they leave their workstations
- All confidential information, whether contained on written documents or electronically, should be marked as "confidential."
- All confidential information should be disposed of properly (e.g., employees should not print out a confidential document and then throw it away without shredding it first.)
- Employees should refrain from discussing confidential information in public places
- Employees should avoid using e-mail to transmit certain sensitive or controversial information
- Limit the acquisition of confidential client data (e.g., social security numbers, bank accounts, or driver's license numbers) unless it is integral to the business transaction and restrict access on a "need-to-know' basis
- Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed
- Other

7. Availability and Integrity of Information

Information stored on computer systems must be regularly backed-up so that it can be restored if or when necessary.

All care and responsibility must be taken in the destruction of sensitive information. Electronic information relating to customers, administrative and commercial information must be disposed of in a secure manner.

Sensitive or confidential paper documents must be placed in the shredding bins or destroyed in the manner indicated to you by your direct manager.

8. Cybersecurity

[COMPANY NAME] is committed to ensuring the security of its information systems and data and protecting them against cyber-attacks.

Our Company has therefore implemented specific measures to ensure cybersecurity, such as:

Server Configuration Guidelines

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements
- Servers should be physically located in an access-controlled environment
- Servers are specifically prohibited from being operated from uncontrolled cubicle areas

Control Software Installation

- Employees may not install software on computing devices operated within the network
- Software requests must first be approved by the requester's manager and then be made to the IT team in writing or via email
- Software must be selected from an approved software list, maintained by the IT team, unless no selection on the list meets the requester's need
- The IT team will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation

Malware Protection

- All computers must have [COMPANY NAME]'s standard, supported anti-virus software installed and scheduled to run at regular intervals
- The anti-virus software and the virus pattern files must be kept up-to-date
- Virus-infected computers must be removed from the network until they are verified as virus-free
- Any activities with the intention to create and/or distribute malicious programs into [COMPANY NAME]'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited

Mobile Device Encryption
All mobile devices containing stored data owned by **[COMPANY NAME]** must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, tablets, and smartphones.

Control of Remote Access
- It is the responsibility of employees, contractors and agents with remote access privileges to **[COMPANY NAME]**'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to **[COMPANY NAME]**
- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. At no time should any authorized persons provide their login or credentials to anyone, not even family members
- Regarding the use of Virtual Private Network (VPN), only **[COMPANY NAME]**-approved VPN clients may be used. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks

Cybersecurity Trainings
Employees and data users of **[COMPANY NAME]** are required to regularly complete cybersecurity training sessions. It includes awareness raising on:
- Device loss or theft
- Social engineering tactics
- Phishing
- Malware and ransomware
- Zero-day exploits
- Macro and script attacks
- Botnet attacks

Cybersecurity Testing
In order to test our cybersecurity vulnerabilities, specific tests are undertaken on **[COMPANY NAME]**'s own networks on a regular basis.
These security controls are operated through internal cybersecurity testing and assessment methods / an external Breach and Attack Simulation (BAS) platform, namely [specify the name of your BAS platform].

9. User responsibilities

Any data security system relies on the users of the system to follow the procedures necessary for upholding data security policies. Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to [contact detail and position].

Employees are therefore expected to:

- Comply with data security procedures and policies
- Complete all data security and cybersecurity trainings required by the Company

- Protect their user ID and passwords
- Inform the [contact detail and position] department of any data security questions, issues, problems or concerns
- Assist the [contact detail and position] department in solving data security problems
- Ensure that all IT systems supporting tasks are backed up in a manner that mitigates both the risk of loss and the costs of recovery
- Be aware of the vulnerabilities of remote access and their obligation to report intrusions, misuse or abuse to the [contact detail and position] department
- Be aware of their obligations if they store, secure, transmit and dispose of vital information concerning the activities or operations of the company, customers, partners or strategic information on the company's products and services
- Return company's portable devices (e.g. company-owned laptop, smartphone, USB drive, etc.) before exiting the premises on their final day of employment

10. System Administrator

System administrators, network administrators and data security administrators will have access to the host systems, routers, hubs and firewalls necessary to perform their tasks.

All system administrator passwords will be deleted immediately after an employee who has access to these passwords has been terminated, dismissed or otherwise left the company's employment.

11. Managers Duty

Supervisors / Managers shall immediately and directly contact [specify department or position] to report change in employee status that requires terminating or modifying employee login access privileges.

12. Monitoring information

The company has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is/It is not our company's intent to continuously monitor all computer usage by employees or other users of the company computer systems and network.

However, users of the systems should be aware that the company may monitor usage, including, but not limited to:

- patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access)
- employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with company policy
- other

13. Audit

[COMPANY NAME] uses technologies such as [audit technology] to provide an audit trail over its infrastructure and systems.

Auditing allows ad hoc security analysis, track changes made to **[COMPANY NAME]** setup and audit access to every layer of the stack.

To ensure security of data, **[COMPANY NAME]** will regularly plan audits.
Those audits are to be performed internally by [position in the company] / by a third party [name of the organization].

14. Reporting Incidents

If any individual becomes aware that Company Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this Policy, they are responsible for reporting data breach and information security incidents immediately to [position] ([position email]) within [number of days] business days. **[COMPANY NAME]** shall then process measures to preserve evidence and eliminate the cause of the Data Breach.
If the breach occurs or is discovered outside normal working hours, it must be reported as soon as possible.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to individuals, the nature of the information leaked or stolen and the estimated severity of the breach.

15. Disciplinary Action

All employees are to always follow this policy, and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: the company may issue a verbal warning and train the employee on security
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): the company will invoke more severe disciplinary action up to and including termination

Each incident, both confirmed and suspected, will be examined on a case-by-case basis.

Employees who are observed to disregard the company's security instructions will face progressive discipline, even if their behavior has not resulted in a security breach.

Any third-party partner or contractor found in violation may have their network connection terminated.

16. Revision history table

Every policy revision should be recorded in this section

Version	Date of Revision	Author	Description of Changes

17.Agreement

I acknowledge that I have received a copy of the **[COMPANY NAME]** Data Security policy. I have read and understood the policy. I understand that, if I violate the policy, I may be subject to disciplinary action, including termination. I further understand that I will contact my supervisor if I have any questions about any aspect of the policy.

Dated: _____

EMPLOYEE COMPANY

_____ _____

Authorized Signature Authorized Signature/Company Seal

_____ _____

Print Name and Title Print Name and Title