Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Information security policy for Mentorloop staff

Using this policy

- This policy outlines behaviors expected of employees when dealing with company and customer data and provides a classification of the types of data with which they should be concerned.
- Mentorloop is a data controller and, because it operates in the EU as well as Australia, adheres to the guidelines set out in the General Data Protection Regulation (GDPR).
- This policy applies to all employees, contractors, volunteers, students, graduates and others on work experience, and anyone who has permanent or temporary access to Mentorloop systems, data, or hardware.

Purpose

Mentorloop must protect restricted, confidential, or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data is a critical business requirement, yet flexibility to access data and work effectively is also critical. Regulations, such as the GDPR, also require the protection of a broad scope of data, which this policy supports by restricting access to data hosted on Mentorloop devices.

In scope data

Types of data to be protected:

- Personally identifiable information (PII) - any data that could potentially identify a specific individual of employees, customers, partners, vendors
- Financial - unpublished financial information
- Restricted/Sensitive customer data and customer lists (existing and prospective)
- Confidential company data
- IP - Patents, formulas or new technologies

- Secrets - passwords, API keys, authentication tokens, etc. of Mentorloop and its employees, customers, partners, vendors

From here on, “data” refers to “in scope data”.

In scope systems

- All Mentorloop workstations – desktops and laptops.
- All Mentorloop virtual machines.
- All staff personal devices – computers and phones

From here on, “systems” refers to “in scope systems”.

Mentorloop obligations

Our Network Administrators will:

- Configure staff workstations and personal devices as per the device security policies.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow these policies as other employees do.

Mentorloop has adopted a tiered approach to data security. A group of sensitive data/VIP users is limited to the CEO (Lucy Lloyd) and the CTO (or acting CTO). These users have access to more sensitive, restricted use data, and systems.

Employee requirements

All employees are required to protect data. In this policy, we will give employees instructions on how to avoid security breaches. Carefully read Appendix 1: Mentorloop security awareness quick reference.

Employees should follow instructions to protect their devices and refer to the CEO (Lucy Lloyd) or CTO if they have any questions.

Data Privacy

- Employees must notify the CEO (Lucy Lloyd) if they suspect they are not in compliance with this policy.
- Visitors to Mentorloop must be escorted by an authorized employee at all times. If you are responsible for escorting visitors, you must restrict them to appropriate areas.
- There may be times when there are visitors to the office whom you are unfamiliar with. This is our space, and we need to be vigilant about protecting it. If there is any doubt as to a visitor in the building, and you believe you've identified an unknown, unescorted, or otherwise unauthorized individual in the Mentorloop office, you need to immediately notify the CEO (Lucy Lloyd) or COO (Heidi Holmes). If both are unavailable then notify the CTO.
- You are required not to reference the subject or content of sensitive or confidential data publicly or via systems or communication channels not controlled by Mentorloop. For example, the use of external email systems not hosted by Mentorloop to distribute Mentorloop data is not allowed.
- To maintain information security, you must ensure that printed data is not left unattended at your workstation. Properly dispose of any printed data that is no longer required. Shred documents with sensitive data, including PII.
- When communicating with customers, always verify their identity by emailing them at the address associated with their Mentorloop account. It's easy to fake a from address - you must verify that the customer can receive emails to this address.
- All employees are required to use a secure password on all Mentorloop systems as per the password policy in section 14 of this document. These credentials must be unique and must not be used on other external systems or services.
- Staff must use an individual, personally-identifiable account at all times. Staff must not share access to a single account.
- As an employee, you have a right to request information about yourself held both manually and on computer by Mentorloop. This request must be made in writing and sent to the CEO (Lucy Lloyd). You also have the right to rectify, block, or delete information which is regarded as wrong or incorrect.
- Terminated employees will be required to return all records, in any format, containing personal information.

Handling and transferring sensitive data

Employees should avoid transferring sensitive data (e.g. secrets, customer information, employee records) to other devices or accounts unless absolutely necessary. Data that must be moved within Mentorloop is to be transferred only via business-provided secure transfer mechanisms (e.g. company approved file sharing software, company email). Mentorloop will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle data. If you have a query regarding use of a transfer mechanism, or the provided options do not meet your business purpose, you must raise this with the CEO (Lucy Lloyd).

Employees are required to:

- Share confidential data over the company network/system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches, and hacking attempts.

If there is doubt regarding the requirements, seek guidance from the CEO (Lucy Lloyd).

Email usage

Employees are encouraged to be considerate when sharing their work email addresses and only disclose this to known, trusted sources. Only opening email attachments from trusted contacts and businesses helps block junk, spam, and scam emails. Delete and report suspicious looking emails to the CEO (Lucy Lloyd) or CTO.

Workstations and equipment

Staff requiring access to sensitive information systems will be provisioned with a company workstation.

Workstations must be configured in line with the following policies:

- All user accounts are secured with a strong, unique password
- All guest accounts are disabled
- Automatic login to any accounts is disabled

- Full disk encryption is enabled and the recovery keys are recorded safely and securely
- Devices will automatically lock after a period of 2 minutes inactivity
- Devices require users to login after the screen is locked, screensaver is activated, or laptop lid is closed
- Operating system and application security updates are configured to automatically install
- Applications may only be installed from trusted sources. If you need to install something on your work laptop for work purposes and are unsure about whether it is a trusted software, check with the CTO before installing.
- Any software that doesn't directly relate to a job function must not be installed on company workstations.
- Any software no longer supported by the provider or no longer in use must be uninstalled from company workstations.
- Google Chrome is the preferred browser and should be used as your default on your work laptop.
- Accounts are locked after five failed password attempts are made within ten minutes.

Until the CTO has confirmed that a workstation has been correctly configured with the policies above, it must not be used to interact with any Mentorloop information systems.

Staff may only use personal devices (e.g. phones) to connect to Mentorloop information systems with the express approval of the CEO or CTO. Personal devices must be configured in line with the same workstation policies listed above.

Any devices used to interact with Mentorloop information systems should be used in line with the following policies:

- Strong, unique passwords must be used for all services.
- Multi-factor authentication (MFA) must be enabled for all services that support it.
- Never connect to any Mentorloop information systems on an untrusted device.
- Never connect to any Mentorloop information systems on an untrusted or public network.
- Never put company data on a USB key or external storage device without the express permission of the CEO or CTO.

- Never transfer company data to a system that hasn't been expressly approved by the CEO or CTO (e.g. your personal email address or a Dropbox account).
- Maintain the physical security of your devices; don't leave them in the office overnight or in the back of your car.
- If your workstation or personal device is lost or stolen, report it immediately to the CEO or CTO.
- Any suspicious activity, no matter how trivial, should be reported immediately to the CEO or CTO.
- Mentorloop has the right to access any encrypted device for the purposes of investigation, maintenance, or the absence of an employee with primary file system access.
- All security related events will be logged and audited by the CEO (Lucy Lloyd) to identify inappropriate access to systems or other malicious use.

If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Remote employees must follow this policy's instructions as they would if working in the Mentorloop office. Since they will be accessing company systems remotely, they are required to follow all data encryption, protection standards and settings, and ensure their private network is secure. Seek guidance from the CTO if you are unsure as to your responsibilities.

Using generative AI and other AI tools

AI tools must be approved by management before use to ensure compatibility, security, and compliance with organizational policies and standards. Approved AI tools may be used for legitimate business operation purposes only, subject to the following:

- When using AI tools, agency and accountability for any outcomes or decisions rest with you. Use of generative AI does not release you from your responsibility to act ethically and with consideration of others.
- Do not use excessive or unnecessary data with AI tools, especially PII or any commercially-sensitive data about Mentorloop, that may pose privacy risks to individuals or Mentorloop.
- Use only the minimum amount of data necessary.
- Use AI tools ethically. For example, do not change a person's appearance or modify an image to show an event that did not actually occur.

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Social media and internet access standards

All employees have a responsibility to use the Company's computer resources and the Internet in a professional, lawful, and ethical manner.

Internet use brings the possibility of breaches of the security of confidential company information and creates the possibility of contamination to our system via viruses or spyware. Internet use, on company time, using company-owned devices that are connected to the company network, is authorized to conduct Mentorloop business only.

This part of our staff policy outlines how Mentorloop and its employees should conduct themselves online. It helps safeguard our brand's reputation and provides guidelines for employees to responsibly share the company's message should they wish.

- Employees should carefully consider what is appropriate business information to share on social media channels - proprietary, sensitive, personal, protected, financial, customer, or confidential information that is not in the public domain should not be shared on any social channels.
- Use your own personal email address when signing up for social media accounts that are not connected to your role at Mentorloop.
- Some personal use of social media is acceptable at work. You should apply a professional level of discretion when using social media at work for non-work-related purposes and consider carefully which websites and social media channels are appropriate to access during work hours.
- Inappropriate content must not be accessed by employees while at work or while using Mentorloop resources. Likewise, staff must not post inappropriate material using company resources. Employees are expected to use common sense and consideration for others when deciding on content appropriate for the workplace.
- Social media can be a tool for scammers and criminals including phishing scams and ransomware attacks. Employees must be vigilant when it comes to protecting the security of the devices that they use for work.

Security incident reporting

Incidents include:

- Physical security breaches on Mentorloop's premises
- Loss of Mentorloop owned information
- Loss or theft of Mentorloop assets
- Viruses like malware, spyware, ransomware
- Misuse of Mentorloop systems
- Breaches of laws
- System crashes

You must immediately notify the CEO (Lucy Lloyd) or COO (Heidi Holmes) in the event that a device containing PII and company data is lost, stolen, or damaged (e.g. mobiles, laptops, or electronic devices or printed material); and change all account passwords at once when a device is lost or stolen.

In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform the CEO so that they can take appropriate action.

Disciplinary action

- We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:
- First-time, unintentional, small-scale security breach - we may issue a verbal warning and train the employee on security.
- Intentional, repeated, or large scale breaches (which cause severe financial or other damage) - we will invoke more severe disciplinary action up to and including termination.
- We will examine each incident on a case-by-case basis.
- Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Password policy

- Access to information systems and related applications is audited on a regular basis and provisioned/deprovisioned as pertaining to job function.
- Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:
- Choose passwords at least 12 characters long (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g. birthdays) and not contain a complete word which easily links to you including your name, company name, family member or pet.)
- Passwords must be updated every six months and must not be reused. They must be unique from each other and different from previous passwords.
- Remember passwords instead of writing them down. If it is necessary to write down a temporary password, it is a requirement to keep the paper or digital document confidential and destroy it immediately after the password has been used and changed.
- Exchange credentials only when absolutely necessary. When exchanging them in person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to. Use of approved password management tools to transfer credentials is permitted within Mentorloop.
- Use of approved password management tools on Mentorloop devices is permitted. Otherwise, select "no" when a computer offers to automatically remember your password when logging in to a website or application.

Remembering a large number of passwords can be daunting. We have purchased the services of a password management tool (TeamPassword) which generates and stores passwords. Employees are required to create a secure password for the tool itself, following the above mentioned advice.

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Leaving the Organisation

Any organization provided equipment is the property of Mentorloop. When an employee leaves Mentorloop it is their responsibility to make arrangements for the return of all assigned equipment to their Manager or other designated individual. Equipment can include, but is not limited to the following: laptops, USB drives, mobile phones.

Last updated: March 2024

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Appendix 1: Mentorloop security awareness quick reference

Workstations & devices

It is company policy that all workstations and personal devices are configured with:

- User accounts are secured with a strong, unique password
- Guest accounts and auto-login are disabled
- Full disk encryption is enabled
- The device will lock itself automatically after a period of 2 minutes of inactivity
- Security updates are automatically installed

If a new workstation has been provisioned for you or you are bringing your own device, it must be configured and approved by the CTO prior to being used to connect to any Mentorloop information systems.

Personal devices (laptops, phones, etc) may only be used to connect to Mentorloop systems with the express approval of the CEO or CTO, and should be configured in accordance with the staff workstation policy.

Security awareness checklist:

- [ ] Use strong, unique passwords for all systems.
- [ ] Multi-factor authentication must be enabled for all systems that support it.
- [ ] Never connect to any Mentorloop information systems on an untrusted device.
- [ ] Never connect to any Mentorloop information systems on an untrusted or public Wi-Fi or network.
- [ ] Never put company data on a USB device or other external storage device without the express permission of the CEO or CTO.
- [ ] Never transfer company data to a system that hasn't been expressly approved by the CEO or CTO (e.g. to your personal email or Dropbox.)
- [ ] When communicating with a customer, always verify their identity by emailing the email address associated with their Mentorloop account and verifying that they can reply to it. From addresses can be faked - ensure the customer can *receive* emails to the correct address.
- [ ] Maintain the physical security of your devices. Don't leave them in the office overnight or in the back of your car.
- [ ] If your workstation or personal device is lost or stolen, report it immediately to the CEO or CTO.
- [ ] Report anything suspicious, no matter how trivial it may seem.
- [ ] If you're ever unsure about any of the above, ask the CEO or CTO directly.