IT-Regulations

of

Open Home Foundation

TITLE 1. PURPOSE AND SCOPE

Article 1 – Purpose

1. These IT Regulations set out the mandatory and recommended security principles, as well as the rules governing the proper handling of electronic data and IT resources within the Open Home Foundation (**Foundation**).
2. These Regulations are adopted in accordance with article 9 of the Foundation Deed dated 5 September 2024.

Article 2 – Scope

These Regulations apply to all members of the Foundation Board, employees, contractors, consultants, volunteers, and any other individuals who have been granted access to the Foundation's IT resources or who process Foundation data (**Personnel**). References to "employees" in these Regulations shall be construed to include all Personnel unless the context requires otherwise.

TITLE 2. DATA PROCESSING

Article 3 – Data Processing

1. Foundation-related documents and data must be processed exclusively on the Foundation’s IT infrastructure and sent using Foundation-approved communication tools and applications.
2. All documents, information and data belonging to, created by, or held on behalf of the Foundation must be stored on secure and encrypted storage devices or services managed by the Foundation.
3. Foundation documents and data may not be forwarded to private or third-party email accounts or devices.
4. Requests for the use of Foundation-unapproved IT tools and services must be submitted to and approved by the Foundation IT staff before use.

Article 4 – Use of Data Processing and Communication Equipment

1. All devices used for work at the Foundation must be locked when not in active use to prevent access by third parties.
2. This also applies to short absences from the workplace. All devices must be automatically locked by the operating system of the device after a maximum of three minutes of inactivity.
3. The use of public or unsecured Wi-Fi networks is prohibited without the use of additional encryption using secure VPN software. Employees must use secure encrypted network communications when travelling. For convenience, secure VPN software is provided to all Foundation employees.
4. To exchange sensitive data within the Foundation, including but not limited to personal data, client data and passwords, only specialized secure communication and sharing software is allowed. Email and chat services are not considered secure communication tools. The Foundation provides a secure communications tool for this purpose to all employees.

TITLE 3. IT INFRASTRUCTURE

Article 5 – Office Equipment

All IT equipment which is the property of the Foundation must be handled with appropriate care.

Article 6 – Laptops

1. All employees are offered a computer of their choice to use for their work at the Foundation, as long as its costs are within the limits of the budget provided.

2. Where possible, the Foundation offers a 3-year extended warranty to cover repairs for the laptops owned by the Foundation.
3. If extended warranty is not available for the laptop of choice of the employee, any future repair will be funded out of the equipment budget assigned to the respective employee.
4. Laptops owned by the Foundation are intended primarily for Foundation use.
5. The employee is responsible for maintaining the laptop's operating system and other software, applying all available security updates, and ensuring all software used is fully supported by its vendors and maintainers.
6. The storage of private data on the laptop is at the user's own risk. The Foundation accepts no liability whatsoever for private data stored on a laptop of the Foundation and the Foundation will make no effort to rescue such data.
7. The laptops owned by the Foundation must be returned to the Foundation if the employee stops working for the Foundation, unless the employee chooses to purchase the laptop from the Foundation.
8. If the laptop is purchased by the employee, all Foundation data must be erased immediately.
9. If the laptop is returned to the Foundation, its contents may be deleted within twelve months after the return.
Article 7 – Privately Purchased Computers
1. Employees have the option to decline the computer offer and use their privately owned computer instead, as long as it fully complies with all aspects outlined in these Regulations.
2. The Foundation assumes no responsibility and provides no support for privately owned computers used for work at the Foundation.
3. As soon as the laptop is no longer being primarily used for the Foundation, all Foundation data must be erased immediately.
Article 8 – Mobile Phones
1. Where in the interest of the Foundation, the Foundation, at its sole discretion, may grant some employees a mobile phone budget for professional purposes.
2. Where in the interest of the Foundation, a SIM card or e-SIM can be provided by the Foundation on request and used in privately owned mobile phones.
3. Foundation employees are allowed but not required to use their privately owned mobile devices for their work at the Foundation.
4. All mobile devices used for work at the Foundation must comply with the requirements in these Regulations, regardless of ownership by either the Foundation or the employee. This includes the requirements for encrypted storage and the use of VPN networks when travelling.
5. Foundation employees are responsible for continuously updating the operating system and apps running on their mobile devices when used for their work at the Foundation. The device should be supported by its vendor and security updates must be readily available and installed promptly when made available.
6. If a privately owned mobile phone is lost or broken, costs to replace or repair the phone will be at the expense of the employee concerned.
TITLE 4. AUTHENTICATION
Article 9 – Principles

1. Employees are required to use MFA (Multi-factor Authentication) methods when logging in to essential Foundation infrastructure, applications and devices where possible. MFA means that at least two authentication methods must be used. These include the following options:
    a. Physical authentication devices such as Yubikeys or similar.
    b. Biometric authentication such as fingerprint, face recognition or iris scan.
    c. OTP (One Time Password) as provided by various Authenticator apps and password manager apps.
    d. Passkeys.
    e. Asymmetric Encryption key pairs.
    f. Unique strong passwords.
2. All employees are required to use a secure password manager application for all authentication where other MFA options are not available. The Foundation provides such a secure password manager application to all employees.
3. All employees are offered a pair of physical authentication devices.

Article 10 – Sharing Passwords and other Sensitive Data

1. Authentication credentials must not be shared. Individual accounts must be used at all times.
2. In exceptional cases where authentication credentials or other sensitive personal data needs to be shared between Foundation employees the password manager application provided by the Foundation should be used.
3. Sharing or storing authentication credentials in any other way is strictly prohibited.

Article 11 – Strong Unique Passwords

1. Foundation employees must secure their password manager account with a unique strong password that they can easily memorize as well as at least one other authentication method.
2. Passwords should never be re-used, not even partially. This makes them unique and avoids security issues when one personal account is compromised and its credentials are used to access that same person's account on other services or devices.
3. All employees are encouraged to use passwords that comply with the following best practices:
    1. Avoid using names, first names, date of birth, telephone extensions, etc. as passwords.
    2. String multiple totally unrelated words together into a very long password.
    3. Avoid adding an incremental number and an exclamation mark at the end of a universal password.
    4. Avoid using 1337 speak (substituting letters for numbers), as this is easily predictable.
    5. Aim for creative and unpredictable passwords.
4. If an employee suspects that a third party has obtained their password, it must be changed immediately and the Foundation’s IT team informed.

TITLE 5. INTERNET

Article 12 – Safe Use of Internet

1. All employees must ensure their Internet connections are secure and encrypted. Secure encrypted network connections must be used when travelling outside of the employee’s office or home office network or when roaming on foreign cellular networks.
2. In any case, the use of pages with illegal content is prohibited.

3. All Foundation employees must maintain all security features of their Internet router, laptop and Internet applications such as their browser.

Article 13 – Email Account

1. The Foundation email address is to be used for business correspondence. A private email address must always be used for private correspondence.

2. For security reasons, the Foundation's email service scans emails to protect against email attacks. Emails which are blocked can be released by the users themselves. Employees should only do so when they have personally verified the legitimacy of the origin. When in doubt, employees must contact the Foundation's IT team at ict@openhomefoundation.org or reach out to them in #backoffice-ict in chat.

Article 14 – Social Engineering

1. Foundation employees must be cautious of social engineering attacks. Social engineering is the manipulation of people to gain unauthorised access to confidential information or IT systems. Such an attack is usually carried out by telephone or e-mail. Social engineers like to impersonate employees, customers or members of IT support. The victims are deceived by internal company knowledge or knowledge of special technical terms that the attackers have previously acquired through telephone calls or conversations with other colleagues.

2. For requests for password or username disclosure via email or over the phone, employees must contact the Foundation's IT team at ict@openhomefoundation.org or reach out to them in #backoffice-ict in chat.

TITLE 6. EXTERNAL DATA ANALYSIS AND PROCESSING

Article 15 – Principle

With regard to external data analysis and processing tools (for example for the generation of text or images, or the generation, management or analysis of documents – with or without AI support), the following principles apply:

a) the use of tools that are explicitly approved by the Foundation (for example, MS Copilot or DeepL Pro); and
b) the use of tools that are not explicitly approved by the Foundation (for example, ChatGPT) is not prohibited, but such tools must be used strictly without any sensitive data such as personal or confidential data (i.e. completely sanitized and anonymized).

TITLE 7. INCIDENT REPORTING AND RESPONSE

Article 16 – Incident Reporting

1. An "IT Security Incident" includes any event that may compromise the confidentiality, integrity, or availability of Foundation data, systems, or devices. This includes, in particular:

a) loss or theft of a laptop, mobile phone, storage device, or any other equipment;
b) suspected or actual malware infection (virus, ransomware, spyware, etc.);
c) unauthorised access or attempted access to accounts, systems, or files;
d) unusual system behaviour or suspected phishing emails;
e) misdirected emails containing confidential information;
f) any breach or suspected breach of these Regulations.

2. Employees must report any suspected or confirmed incident immediately, and in any event within 24 hours of becoming aware of the incident, to the designated Foundation IT contact at ict@openhomefoundation.org. If the incident involves personal data, the report must be made without undue delay to enable the Foundation to comply with applicable data protection notification requirements. If the incident involves loss, theft of equipment, or any other criminal activity, local law enforcement must be notified as required.

3. Employees must report even suspected incidents. Employees must not attempt to fix or investigate incidents themselves (e.g., deleting suspicious files, running unapproved tools).
Article 17 – Incident Response
1. Upon receiving a report, the Foundation will take appropriate measures to contain the incident.
2. The Foundation will investigate the cause, scope, and potential impact of the incident, including whether personal or confidential data has been compromised.
3. When necessary, the Foundation will take further corrective measures.
Article 18 – Cooperation Duty
1. Employees must cooperate fully during incident investigations.
2. Employees must provide all relevant information and, if necessary, surrender affected devices for inspection.
3. Failure to report an incident or cooperate with an investigation may lead to disciplinary consequences in accordance with Foundation procedures.
TITLE 8. MONITORING OF CORRESPONDENCE, INTERNET BEHAVIOUR, DATA DOWNLOADING AND SENDING
Article 19 – Emails
An employee who leaves the Foundation must clean up his or her email account and delete all purely private data. Business emails may not be deleted.
Article 20 – Data Extract
1. Log files may be generated by the Foundation's systems and services. The Foundation may evaluate and analyse such data by user if required. This includes an evaluation of the opening, downloading, and sending of files.
2. All work results and the rights thereto belong to the Foundation. The editing, sending and other use of the Foundation's work results for purposes other than for the purpose of fulfilling the employment relationship with the Foundation are not permitted.
TITLE 9. FINAL PROVISIONS
Article 21 – Implementation and Modifications
These Regulations are subject to periodic review and may be updated by the Foundation Board. Any amendments will be communicated in a timely manner.
Article 22 – Effective Date
These Regulations enter into force upon adoption by the Foundation Board.

The Foundation Board of Open Home Foundation:

Chairman of the Foundation Board

Brooklyn 6/23/2026

Signed by:
Paulus Schoutsen
6C624E7D4571416...

Ort, Datum / Place, date

Paulus Schoutsen

Member of the Foundation Board

Neuheim 6/25/2026

Signiert von:
283FDEB2404B424...

Ort, Datum / Place, date

Pascal Vizeli

Member of the Foundation Board

Houston 7/1/2026

Signed by:
John Nelaus Koston
22F7335E7EFA434...

Ort, Datum / Place, date

John Koston

Member of the Foundation Board

Versailles, KY 6/23/2026

Signed by:
Trevor Schirmer
614CE8DED6E54C7...

Ort, Datum / Place, date

Trevor Schirmer