YOUR TRUSTED SECURITY PARTNER

Document:	Information Security Policy
Date:	09/04/2026
Approver's name:	Emanuel Prenga
Approver's title:	Director
Approver's signature:	
Next review due:	09/04/2027
Policy owner:	Director

- All staff are fully aware of company's policies and procedures, including their confidentiality and nondisclosure duties following the use of the company's network, software, facilities and documents. Areas of responsibility are clearly defined without any Conflicting duties (Job descriptions)
- To mitigate the risks of viruses, malware and data loss:
    - Company's network is managed and controlled by an IT specialist.
    - Critical data and system configurations are backed up on a regular basis and stored in a safe place.
    - Installation of software by users is restricted, as only the IT specialist has admin control over network.
    - Staff must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. They must delete spam, chain, and other junk email without forwarding.
- To prevent unauthorized access to systems and applications:
    - A secure log-on procedure is in use for all users.
    - All computing devices are secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. All users must lock the screen or log off when the device is unattended.
    - Laptops and mass storage devices such as CDROM, DVD or USB drives must be either locked with a locking cable or locked away in a drawer.
    - Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location
- To prevent unauthorized access to sensitive/confidential information in hardcopy form:
    - Staff are required to ensure that all sensitive/confidential information in hardcopy form is secure in their work area by removing them from the desk and locking them in a drawer when the desk is unoccupied and at the end of the work day.
    - File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended. Keys used for access to restricted or sensitive information must not be left at an unattended desk.
    - Printouts containing restricted or sensitive information should be immediately removed from the printer.
    - Upon disposal restricted and/or sensitive documents should be shredded
    - Whiteboards containing restricted and/or sensitive information should be erased

Secure Frontline Services Ltd is registered in England & Wales. Company Reg No: 5422196
First Floor Offices
120 High Road, London, N2 9ED
0870 479 8512
0870 479 8513
mail@securefrontline.com
www.securefrontline.com

- In order to evaluate the compliance with this policy, the director will implement various methods:
    - Periodic walk-thrus
    - Business reports in monthly management meetings
    - Internal audits within yearly Data Protection Risk Assessment
    - Feedbacks from staff. Any information security events are to be reported to the director as quickly as possible.
- When a nonconformity occurs, the organization take action to control and correct it

This Policy is reviewed annually, or upon legislative updates.

Secure Frontline Services Ltd is registered in England & Wales. Company Reg No: 5422196
First Floor Offices
120 High Road, London, N2 9ED
0870 479 8512
0870 479 8513
mail@securefrontline.com
www.securefrontline.com