Great Family Organization

Security Procedure Manual

Introduction

Great family Organization (GFO) security procedure includes the standardised processes and guidelines that GFO follows to protect its assets and information. These procedures outline the steps to be taken to prevent, detect, and respond to security incidents. GFO's security procedures seeks to reduce risk exposure while improving regulatory readiness and operational efficiency.GFO's security procedures form the backbone of all GFO's security policies that enable growth with confidence.

The Objectives of GFO's Security Procedures

- Clear task assignments
- Reduced liability
- Stronger internal controls
- Improved stakeholder trust

When designed correctly, security measures and procedures protect organizational resources while enabling secure access, collaboration, and decision-making.
GFO Security Responsibilities

The extent to which GFO put security arrangements and procedures in place vary. However, GFO has legal responsibilities to ensure security risks are managed in the workplace.

Physical Security

GFO's physical security policy covers all aspects of securing GFO's office premises, including:

- Access control systems and ID verification
- Surveillance cameras and alarms
- Fire prevention and emergency response plans
- Visitor management and employee tracking
- Protection of physical assets (e.g., laptops, desks)

Audience

The GFO's Physical Security Policy applies to all individuals that install, support, maintain, or are otherwise responsible for the physical security of (GFO) Information Resources.

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
- Physical access to all (GFO properties) restricted facilities must be documented and managed.
- All **Information Resource** facilities must be physically protected in proportion to the criticality or importance of their function at GFO.
- Access to **Information Resources** facilities must be granted only to GFO's personnel and contractors whose job responsibilities require access to that facility.
- All facility entrances, where unauthorized persons could enter the premises, must be controlled.

- Secure areas must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This includes:
  - information processing facilities handling **confidential information** should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
  - **controls** should be adopted to minimize the risk of potential physical and environmental threats;
  - environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.
- Equipment must be protected from power failures and other disruptions caused by failures in utilities.
- Restricted access offices and locations must have no signage or evidence of the importance of the location.
- All **Information Resources** facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card access records and visitor logs for **Information Resource** facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Visitors in controlled areas of **Information Resource** facilities must be accompanied by authorized personnel at all times.
- Personnel responsible for **Information Resource** physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Access Control

GFO's Physical Security establish the rules for the granting, control, monitoring, and removal of physical access to (Company) Information Resource facilities. The outline procedures for granting, monitoring, and revoking access to facilities. This includes t he use of ID badges, biometric systems, and visitor management protocols.

- The process for granting card and/or key access to Information Resource facilities must include the approval of physical security personnel.
- Each individual that is granted access to an **Information Resource** facility must sign the appropriate access and non-disclosure agreements.
- Cards must not be reallocated to another individual, bypassing the return process.
- Physical security personnel must remove the card and/or key access rights of individuals that change roles within (Company) or are separated from their relationship with (Company).
- Physical security personnel must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

Physical barriers

Describe the physical security measures in place, such as fences, gates, and security personn el, to prevent unauthorized access.

- All utility systems in use at the facility must be identified and documented with detailed procedures for overall maintenance requirements.
- Maintenance and testing activities must be performed in accordance to manufacturers specifications and must be documented to provide an audit trail of all activities.
- Utility systems must be secured from unauthorized access.
- Utility systems must be set to alarm on malfunctions.
- Emergency systems, lighting, fire suppression, and emergency power systems, must be in place and tested regularly to ensure functionality.
- Critical utilities must be configured in a redundant manner to ensure continued functionality.

Surveillance

Surveillance: Detail the use of cameras and monitoring systems to oversee critical areas and ensure compliance with security protocols.

Incident Response

Establish procedures for responding to security breaches, including reporting mechanisms and emergency contacts.

Capacity building

Training and Awareness: Include guidelines for training employees on security protocols and the importance of maintaining a secure environment.

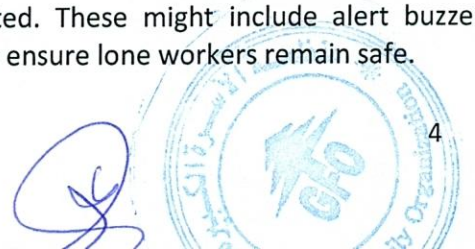
Carrying Out Security Risk Assessments

GFO has a responsibility to carry out its own risk assessment to determine what security measures are needed, whilst ensuring that they are compliant with the law.

This may include things like looking at possible vulnerable locations within the premises. GFO will also be making contingency plans in the event of an emergency situation. Identifying any security measures which need installing and having some way of monitoring these to gauge their effectiveness is also vital.

Training Employees to be Aware of Security Responsibilities

Training also be carried out so that workers are fully aware of their responsibilities should their security be threatened. The resources they have at their disposal to keep themselves safe should also be highlighted. This is important in field where security might be implemented. These might include alert buzzers, toughened glass screen partitions, or systems to ensure lone workers remain safe.



Security in Restricted Areas

Procedures should be put in place and all GFO's staff made aware of them regarding control of access to the premises by visitors. All GFO's staff should be aware where visitors can and cannot go. this include employing the security personnel and installing CCTV cameras, alarms and light systems. Other steps might include having locked access doors for staff, and having regular security checks carried out.

Housekeeping (if third party)

- Housekeeping/cleaning staff must go through standard **information security awareness**
- Where external or third parties are used for cleaning services, the third party must be insured and bonded.
- Housekeeping/cleaning staff must have adequate and approved background checks performed.
- Housekeeping/cleaning staff must be (supervised/monitored) while performing required duties.
- Housekeeping/cleaning staff must wear uniforms, badges, and be assigned a unique identifier that provides an audit trail on access to areas of the facility.
- If housekeeping/cleaning staff need to gain access to restricted areas specific clearance from security staff must be obtained.

Loading Docks

- Procedures for delivery and receipt of packages must be documented.
- Delivery areas must be secured and isolated from public areas.
- External doors of the delivery area must be secured when internal doors are open.
- Delivery areas must be locked when unattended. Unauthorized personnel must be accompanied at all times within delivery areas.
- Surveillance cameras must be secured and adequately cover delivery areas.
- Incoming deliveries must be registered, isolated, and inspected for evidence of tampering before being moved to internal areas.
- All discovered evidence of tampering must immediately be reported to physical security personnel.

Infrastructure Security Policy

Protecting your organization's infrastructure is essential for maintaining business continuity and preventing service disruptions. Your infrastructure security policy should cover:

- Web application firewalls (WAF) and virtual private networks (VPNs)
- Application programming interface (API) security
- Intrusion prevention systems (IPS) and wireless security
- Cloud security, including data storage and cloud-based processes

4. Health and Safety Policy

Ensuring the health and well-being of your employees is not only a moral obligation but also a legal requirement. Your health and safety policy should include:

- Vaccine verification and health checks
- Touchless technology and sanitization protocols
- First aid procedures and training
- Ergonomic workstations and employee wellness programs
- Policies around chemicals, drugs, or other hazardous materials

5. Crisis Management Policy

No organization is immune to unexpected crises, whether it's a natural disaster, a cyber attack, or a public health emergency. Your crisis management policy should outline:

- Disaster recovery and business continuity plans
- Emergency response procedures and communication channels
- Employee evacuation and shelter-in-place protocols
- Post-crisis support and resources for affected employees

- Implementing these essential security policies and procedures is just the first step. Regular training, updates, and assessments are necessary to ensure that your organization remains protected against evolving threats. By prioritizing workplace security, you can create a safe and secure environment for your employees, safeguard your critical data, and maintain the trust of your customers and stakeholders.
- To learn more about developing a comprehensive workplace security strategy, check out our hybrid work security eBook.