

OPSEC POLICY

EDGE GROUP OPERATIONAL SECURITY



1

OPERATIONAL SECURITY OVERVIEW

EDGE Group Operational Security (OpSec) is a function responsible for providing security services and physically protecting all EDGE Group's assets from unauthorised interference.

2

PHYSICAL AND ENVIRONMENTAL SECURITY

The EDGE Group OpSec Policy aims to maintain effective physical and environmental security, and prevent unauthorised physical access to the Group's facilities, while maintaining security of all assets (people, information, and equipment).

There are **three main security areas and controls** that we have to be focused on:



POLICY



SECURE AREAS



EQUIPMENT

2.1 POLICY

The EDGE Group OpSec Policy aims to:

- Demonstrate our Management's commitment to the Group's security;
- Provide guidance on day-to-day operations;
- Prevent unauthorised access and misuse of the Group's information, and information processing facilities;
- Prevent the loss, damage, theft or compromise of assets and interruption to the Group's operations.

The successful implementation and progression of the regulations is a shared responsibility among all of us.

All EDGE Group Entities and sites, including subsidiaries and joint ventures, where the Group holds a majority stake and exercises management control.

All full-time, part-time, temporary staff, contractors, consultants, interns, etc. employed by, or working for, or on behalf of EDGE Group and its Entities.

All other individuals and groups that have been granted access to EDGE Group's content, premises, and Information and Communications Technology (ICT) facilities.

2.2 SECURE AREAS

Secure areas are sites or parts of sites where sensitive information is handled or housed. Buildings, rooms, and offices can all be secure areas. Clearly-defined secure areas will help avert threats and vulnerabilities arising from unauthorised access, destruction of equipment or media, and tampering with security controls. Keep in mind the classification: **GENERAL, SECURED, RESTRICTED, AND SECRET.**

We need to implement and maintain strong and effective:

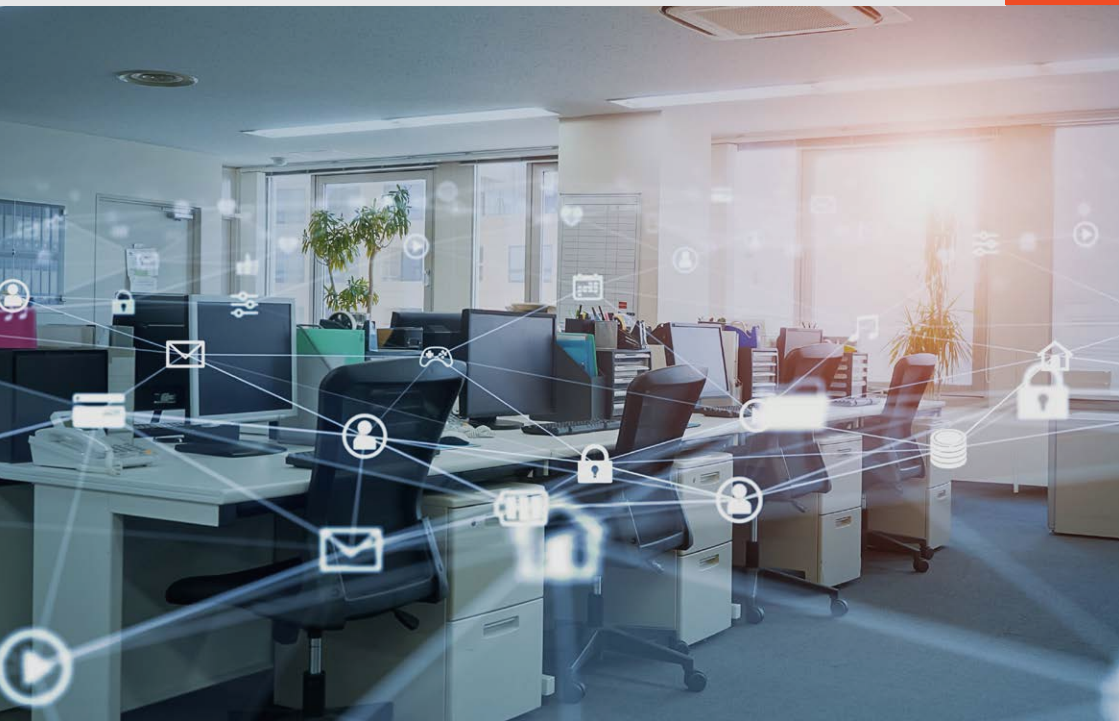
- Physical security perimeters
- Physical entry controls
- Security of offices, rooms, and facilities
- Protection against external and environmental threats
- Work regulations in secure areas
- Public access for visitors, delivery, and loading areas

2.3 EQUIPMENT SECURITY

Effective equipment security prevents loss, damage, theft or compromise of assets and interruption to our activities. Having effective security controls for our equipment will help us prevent threats and vulnerabilities arising from equipment failure, tampering with equipment, and physical theft of assets.

The following measures are to be maintained and implemented effectively:

- Equipment sitting and protection
- Supporting utilities security
- Cabling security
- Equipment maintenance
- Security of equipment off premises
- Secure disposals or re-use of equipment
- Removal of property regulations
- Unattended user equipment regulations
- Clean desk and clear screen policy or approach



3

HUMAN CAPITAL SECURITY

Various security measures are designed with purpose to protect our employees, which is in the essence of our existence and success. Therefore, we must protect our most valuable asset. This is achieved through active security screening and education through various trainings and awareness campaigns.





4

SECURITY MANAGEMENT

Security management includes all aspects of safeguarding our assets. It is focused on continuous monitoring, assessments, and improvements of our security posture through frequent security testing and evaluation of security controls in the areas of:

- Incident Response Management – IRM
- Security Operation Centre - SOC
- Third Party Security Management
- Security Guard Management
- Business Travel Management
- Visitor Management



5

COMPLIANCE, PERFORMANCE EVALUATION AND IMPROVEMENT

We urge you to comply with OpSec's regulations. Within the context of this Policy compliance, performance evaluation refers to the comparison between the outlined requirements and the actual state of implementation of these requirements within Entities and / or sites. The evaluation results will be used to continuously improve.





6

EDGE GROUP SECURITY OPERATION CENTRE

OUR CONTACT INFORMATION

EDGE Group Operation Centre (SOC) is available 24/7 via the below channels:

opsec@edgegroup.ae

800 OPSEC (67732)

Scan the QR code to save the contact details

Security is a group effort. Make sure to report any suspicious activities.