ACCEPTABLE USAGE POLICY

Prepared By:	Egla Taye	Manager Governance, Risk & Compliance	Egla Taye
Reviewed By: **(For Content Validation)**	Georges DeMoura	Vice President, Information Security	Georges De Moura
Reviewed By: **(For ISO Compliance)**	Radha Krishnan	Director Business Excellence	Radha Krishnan
Endorsed By:	Trais Al Ketbi	President, Business Support Services	
Approved By:	Mansour Al Mulla	Managing Director & Chief Executive Officer (CEO)	

STATEMENT OF CONFIDENTIALITY

All information in this document is for the internal use of the EDGE Group only and classified as RESTRICTED information as defined in the Data Classification & Handling Policy.

The information in this document may contain trade secrets, confidential and proprietary information of EDGE Group, the disclosure of which could provide substantial benefit to competitors. As a result, this document should not be disclosed, used or duplicated – in whole or in part without the explicit authorization of EDGE Group management.

The information is intended solely for the use of authorized recipients. If you are not the intended recipient, you are prohibited from reading, using, disseminating, distributing and/or copying this document.

In accessing the document, the reader warrants that the information contained herein will be treated for internal use only and that no content of any nature will be shared with any other external party or unauthorized recipient.

The EDGE logo is a trademark of EDGE Group.

TABLE OF CONTENTS

1. REVISION LOG

All revisions to this document shall be recorded in this Revision Log. Each time a revision is recorded, the Revision Log's control No. will be revised accordingly.

Revision No.	Date	Revision Details	Reason For Revision	Page No.
0	01/07/2023	Initial release	Not applicable	All

2. PURPOSE

EDGE Group has developed and implemented an Information Security Management System (ISMS), which outlines the systematic planning and implementation of security controls to ensure the protection of EDGE Group's information and information assets. The ISMS emphasizes continual improvement of the management system through assurance and review activities on implemented information security controls.

Additionally, EDGE Group is designated as a critical organization and as per the UAE Critical Information Infrastructure Protection (CIIP) Policy, is mandated to adhere to the UAE Information Assurance ("IA") Regulation and apply its requirements to raise the level of protection of information assets and supporting systems across all entities in the Group. This includes information in physical or electronic form that may be owned, leased, or otherwise in the possession, custody, or control of the entities. This CIIP Policy is mandated by the UAE IA Regulation and hence, this policy and its contents are mandatory for EDGE Group.

The purpose of this Acceptable Usage Policy is to establish acceptable use of information assets within EDGE Group and protect both employees and the company from information security risks.

Inappropriate behaviour, especially inappropriate usage of information and information assets by employees or third-party personnel (hereinafter together referred as to "users") can put EDGE Group at risk and lead to loss or damage to EDGE Group's operations as well as reputation. Therefore, it's essential for users to act in a secure, responsible, ethical and lawful manner according to the requirements of this Policy.

3. SCOPE

This Acceptable Usage Policy is applicable to all authorized individuals with access to EDGE Group's information assets.

4. POLICY STATEMENTS

EDGE Group shall ensure:

- Security requirements on permitted and acceptable use of its information and information assets are outlined and users are aware of their responsibilities.
- Secure use of information and information assets to minimize exposure to cybersecurity risks.

4.1 GENERAL REQUIREMENTS AND RESPONSIBILITIES

4.1.1 Ensure protection of EDGE Group's information assets (electronic & non-electronic) including, but not limited to laptops, workstations, portable devices, media, equipment, information and

4.1.2 Only authorized software, information systems and file transfer services shall be used for the exchange of EDGE Group's information.

4.1.3 Users shall be accountable and responsible for activities performed on EDGE Group's assets and services.

4.1.4 User activities shall be logged and monitored for security, legal, compliance and other legitimate purposes. EDGE Group is committed to respecting the rights of its users, including reasonable expectation of privacy.

4.1.5 Users shall not engage in activities that are in violation of information security policies or applicable laws and/or regulations. These activities include, at a minimum:

4.1.5.1 Attempting to gain unauthorized access;

4.1.5.2 Impersonating others;

4.1.5.3 Sharing confidential information with unauthorized parties;

4.1.5.4 Using company-provided accounts to make fraudulent offers on products, items or services;

4.1.5.5 Violating Intellectual Property Rights; and

4.1.5.6 Misusing email and internet services.

4.1.6 Users shall be familiar and comply with applicable information security policies and procedures while using its information systems or services.

4.1.7 Users shall not make unauthorized modifications, disable or override security controls, configured on devices or equipment in their custody. Only authorized IT personnel are allowed to perform maintenance, updates and other technical support activities.

4.1.8 Users shall not use EDGE Group's assets to engage in any fraudulent activities, procuring or transmitting material that is deemed as obscene, offensive or illegal.

4.1.9 Users shall adhere to the EDGE Group's Operational Security Policy for physical and environmental security requirements for information assets.

4.2 HUMAN CAPITAL SECURITY

4.2.1 Security clearance and background checks shall be performed for users requiring access to its information assets.

4.2.2 Confidential agreements and Non-Disclosure Agreements (NDAs) shall be mandatory for all users accessing information assets.

4.2.3 New hire orientation shall include information security training and users shall participate in periodic information security training and awareness sessions.

4.2.4 Information about employees shall not be shared with unauthorized parties without a business purpose and approval from the Information Security and Human Capital (HC) departments.

4.2.5 Users shall adhere to contractually mandated confidentiality requirements.

4.3 INFORMATION ASSET MANAGEMENT

4.3.1 Information assets that are in users' custody shall be returned upon the end of employment or contract.

4.3.2 Information assets taken in and out of EDGE Group's premises shall be declared with the security team and the necessary gate pass shall be obtained with authorizations from relevant departments.

4.3.3 Users shall classify, label and handle EDGE Group's information in accordance with the Data Classification Policy.

4.3.4 Users shall exercise caution in handling information assets while traveling and in public areas outside of EDGE Group's premises.

4.3.5 Users shall immediately report lost, damaged or faulty information assets to the IT Helpdesk.

4.4 WORKSPACE SECURITY

4.4.1 Users shall strictly follow requirements enlisted in the Operational Security Policy, including:

4.4.1.1 Lock workstations when leaving devices unattended and log out from all the applications and systems on a daily basis.

4.4.1.2 Store portable devices and documents securely in office cabinets as and when required.

4.4.1.3 Ensure mass storage devices such as USB drives are securely stored and not left unattended.

4.5 USER ACCOUNTS AND PASSWORDS

4.5.1 Users shall be accountable and responsible for the safety and security of assigned credentials. Sharing of accounts and credentials is not authorized.

4.5.2 Users shall immediately change account passwords if there is a suspected case of credentials being disclosed.

4.5.3 User accounts that have been inactive for more than 30 business days shall be disabled.

4.5.4 Privileged user accounts that have been inactive for more than 30 days shall be disabled.

4.5.5 Users shall not write or store passwords in plain text.

4.5.6 Users shall use different passwords for business and personal accounts.

4.5.7 Users shall always use strong passwords and not utilize commonly known information in passwords (such as pet names, family member names, birth dates, etc.).

4.6 NETWORK AND INTERNET SECURITY

4.6.1 Users shall not connect unauthorized devices to EDGE Group’s corporate network. However, visitors' or users’ personal devices may be allowed to connect to the guest network after obtaining appropriate authorization.

4.6.2 Users shall not engage in any activity that interferes with the normal operation of information systems and services.

4.6.3 Unauthorized network scanning, or attempts to bypass security controls, intercept data, or engage in activities that may result in service disruption are prohibited.

4.6.4 Access to unauthorized websites and services shall be blocked. Users shall contact the IT Service Desk to request for whitelisting of a website or a service based on a business need.

4.6.5 Monitoring and logging network activities shall be in place for security, legal and compliance purposes.

4.6.6 Affecting security breaches or disruptions of network communication is prohibited. Security breaches include:

4.6.6.1 Accessing data of which the user is not an intended recipient; and

4.6.6.2 Logging into an information asset that the user is not explicitly authorized to access.

4.7 COMMUNICATIONS

4.7.1 Users shall ensure EDGE Group’s email and collaboration services are used only for business purposes.

4.7.2 Users shall not forward business emails to personal accounts.

4.7.3 Users shall include only EDGE Group approved signatures and disclaimers in emails.

4.7.4 Users shall only utilize email accounts they are authorized to use.

4.7.5 Ensure that communication considers religious, cultural, political and moral values of communicating participants.

4.7.6 Users shall never exchange messages containing:

4.7.6.1 Defamatory, racist, obscene or otherwise offensive remarks;

4.7.6.2 Malicious attachments, links to malicious or illegal content;

4.7.6.3 Forwarded mail chains usually containing hoaxes, jokes etc.; and

4.7.6.4 Highly Confidential information irrespective of its forms and means.

4.7.7 Attempting to open suspicious emails with attachments or links are prohibited. Users shall immediately report such incidents to the IT Help desk.

4.7.8 Users shall never register with their EDGE Group's email ID on external websites, such as non-work-related discussion boards, mailing lists or other non-business-related websites.

4.7.9 Users shall ensure emails containing sensitive information are encrypted prior to sending.

4.7.10 Forging of email headers, content, spoofing and phishing shall be strictly prohibited.

4.7.11 Email attachments containing sensitive information shall be password protected and the password is shared with the recipient using a different communication channel.

4.7.12 Users shall be aware that they are provided with a fixed amount of mailbox space and their emails are periodically archived to ensure uninterrupted operations.

4.7.13 Use only EDGE Group's authorized secure file transfer services for transfer of documents above the email attachment size limit.

4.8 SOCIAL MEDIA

4.8.1 Posting/communicating/expressing personal views on behalf of EDGE Group and/or any of its users and clients via social media is strictly prohibited unless explicitly authorized.

4.8.2 Disclosing/posting any information on social media platforms that could impact the EDGE Group's reputation is not allowed.

4.8.3 Do not create personal or official social media accounts using EDGE Group's email address.

4.8.4 Users shall ensure online activities do not interfere with job responsibilities and commitments.

4.9 SOFTWARE USAGE

4.9.1 Users shall only use EDGE Group authorized software and applications for official EDGE Group business.

4.9.2 Users shall always contact IT Help desk to request for authorized software installation.

4.9.3 Users shall not install and/ or use software that is not on the approved software list. Downloading free software from the internet or using unauthorized/pirated software for work-related tasks or on EDGE Group information assets is strictly prohibited

4.10 MOBILE AND PERSONAL DEVICE SECURITY

4.10.1 Users requiring EDGE Group related information access on personal devices shall obtain necessary authorization and ensure Mobile Device Management (MDM) related security requirements are met.

4.10.2 Personal devices shall be presented to the Information Technology (IT) Department for applicable provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before accessing the EDGE Group infrastructure and/or network.

4.10.3 Users accessing information via personal devices shall maintain the original device operating system and ensure it is up-to-date with applicable security patches and updates as released by the manufacturer and requested by IT.

4.10.4 Rooted or jailbroken devices are strictly forbidden from accessing EDGE Group's information or information systems.

4.10.5 EDGE Group reserves the right to wipe data of personal devices in the below cases if personal devices are used to access EDGE Group information:

4.10.5.1 If a personal device is lost, missing or stolen containing EDGE Group information;

4.10.5.2 User is terminated or resigns from EDGE Group;

4.10.5.3 If data or policy breach is detected;

4.10.5.4 If malware or similar threat is detected that impacts the security of EDGE Group's.

4.10.6 Usage of unauthorized removable media to transfer confidential information is strictly prohibited. Contact IT Help desk for secure removable media for the transfer of EDGE Group information or for use on EDGE Group information assets.

4.10.7 Users shall not connect any unauthorized removable media to EDGE Group's environment. Users shall be held accountable for:

4.10.7.1 Copying sensitive information to any removable media which could cause confidentiality breach;

4.10.7.2 Transmitting malicious code from removable media to EDGE Group's network;

4.10.7.3 Execution of unauthorized software programs from removable media which could potentially lead to security incidents with business impact; and

4.10.7.4 Legal violations.

4.10.8 Sharing of mobile devices, unless authorized for business purposes, is strictly prohibited.

4.10.9 Users shall immediately report the loss of personal devices that may have EDGE Group's information to the IT Helpdesk.

4.11 INFORMATION SECURITY INCIDENTS

4.11.1 Users shall report suspected information security incidents to the IT Help Desk. Information security incidents may include, but are not limited to:

4.11.1.1 Suspicious emails;

4.11.1.2 Hacking attempts;

4.11.1.3 Malware infections;

4.11.1.4 Lost or unattended devices;

4.11.1.5 Unauthorized access to EDGE Group's information systems;

4.11.1.6 Unusual or suspecting behaviour of information systems such as abnormally slow response time; and

4.11.1.7 Any violations of this policy.

4.11.2 Users shall not attempt to handle or resolve information security incidents.

4.11.3 Users shall report physical and environmental security incidents to the EDGE Group's Operational Security Department.

4.12 USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI)

4.12.1 Users shall be trained on the appropriate use of the GenAI system (including ChatGPT and BARD) and the relevant policies and regulations governing its use.

4.12.2 Employees shall not disclose EDGE Group's confidential or proprietary information to a GenAI technology, directly or through a third-party application without business approval.

4.12.3 Employees shall use GenAI in a respectful and professional manner, refraining from using profanity, discriminatory language, or any other form of communication that could be perceived as offensive.

4.12.4 Employees shall comply with all relevant laws and regulations, including those related to data privacy and information security in accordance with EDGE Group's information security policies.

4.12.5 Employees shall report any security concerns or incidents related to the use of GenAI to the EDGE Group Information Security function.

5. ROLES, RESPONSIBILITIES AND AUTHORITIES

The following table lists the roles and responsibilities of EDGE Group's Policy:

ROLE	RESPONSIBILITIES	AUTHORITIES
Senior Leadership	• Demonstrate commitment to information security by supporting Policy. • Ensure that resources necessary to execute this Policy.	• Resource allocation for policy execution
Information Technology	• Implement necessary controls to ensure technical requirements mandated in this policy are met.	• Managing the EDGE Group network infrastructure, including routers, switches, firewalls, and ensuring network connectivity and security.
Information Security	• With support from the IT Department, develop guidelines that: ○ Identify common practices which may breach EDGE Group's trust and information security policies ○ Define a set of acceptable guidelines that needs to be followed by all the users.	• Setting security standards and enforcing compliance. • Implementing security policies and controls. • Coordinating with other departments to ensure compliance. • Making recommendations for security improvements.
Operations Security	• In coordination with IS and IT Department: ○ Identify common practices that may breach EDGE Group's security policies. ○ Define a set of acceptable guidelines for physical and	• Develop and enforce OPSEC plans, conduct assessments, and provide training to personnel.

ROLE	RESPONSIBILITIES	AUTHORITIES
	personnel security that needs to be followed by all the users.	
Human Capital	• Ensure that: ○ The Policy is shared with all the users at the time of joining. Ensure new joiners sign and accept the policy. ○ Ensure users acknowledge reading the Policy annually. ○ Ensure that the Policy is stored in a location that is accessible by all the employees.	• To enforce the policies and manage workplace behavior.
Line Manager	• Guide and enforce all team members to adhere to the Policy.	• To allocate resources within their department or team. This includes assigning tasks, distributing workloads, and managing budgets for their area of responsibility.
Employees	• Employees and third-party consultants who access information and information assets or use EDGE Group Information Asset shall adhere to this Policy.	• Provide guidance and expertise to those with line authority.
Third-Party consultants		• The scope of work outlined in their contract or agreement.

6. ADHERENCE AND VIOLATIONS

Any violation of this Policy shall be reported to the Information Security department. Violation of this Policy shall be subjected to disciplinary action by EDGE Group's Human Capital Department, taking into consideration the recommendation of the Information Security Department and in accordance with other applicable policies, laws and regulations.

Disciplinary action may range from a verbal warning to discontinuation of access to facility or services, or termination of employment/contract/agreement, and possible legal action. The actual action taken shall depend on factors such as the seriousness of the breach and the user's disciplinary record.

7. COMPLIANCE MATRIX

International Standards Technology (ISO/IEC 27001:2022)	UAE Information Assurance (IA) Standard	Acceptable Usage Policy Section
5.10 Acceptable use of information and other associated assets	T1.2.3 Acceptable Use of Assets	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10
5.24 Information security incident management planning and preparation	T8.1.1 Information Security Incident Management Policy	4.11
7.9 Security of assets off-premises	T1.4.1 Management of Removable Media	4.10

8.5 Secure authentication	T5.5.1 Secure Log on Procedures	4.5
7.6 Working in secure areas	T2.2.5 working in secure areas	4.4
8.1 User endpoint devices	T1.2.4 Acceptable Bring Your Own Device (BYOD) Arrangements	4.10.1, 1.10.2, 4.10.3, 4.10.4, 4.10.5, 4.10.6, 4.10.7, 4.10.8
6.3 Information security awareness, education and training	M3.2.1 Awareness and Training Program	4.2.2

8. TERMS AND DEFINITIONS

TERMS	DEFINITIONS
Authorized Individual	Any individual (employee, third-party, supplier or contractor) who is appropriately vetted and cleared to access information assets for performing or assisting in EDGE Group related business functions.
Information Asset	Refers to information, information content, technology systems and resources used to store, process and maintain information.
Knowledge	Knowledge or data that has value to the organization and is capable of being shared in physical and digital form.
Malware	Malicious software program or file that is intentionally harmful to a computer, network, or server.
Mobile Device Management	Mobile device management (MDM) software allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints.
Personal Device	Non-EDGE Group devices that are owned by employees/non-employees.
Rooted (Android) or “Jailbroken” (iOS) Devices	Modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, e.g., to allow the installation of unauthorized software.
Unauthorized Devices	Information technology devices that are not allowed to access or attempt at accessing EDGE Group resources.

9. REFERENCES

9.1 INTERNAL REFERENCE

S.NO	DOCUMENT NO.	DOCUMENT TITLE
1	--	Nil

9.2 EXTERNAL REFERENCE

S.NO	DOCUMENT NO.	DOCUMENT TITLE
1	--	UAE Information Assurance (IA) Regulation
2	ISO/IEC 27001:2022	Information Security Management Systems Requirements