أدنـوك
ADNOC

ADNOC ACCEPTABLE USAGE OF INFORMATION ASSETS

Declaration

REVISION: R00
DOCUMENT OWNER: GROUP IT FUNCTION
DOCUMENT NUMBER: AHQ/BCS/GIT/ITSRC/FRM/001/R00/19

ص ب 898، أبوظبي، الإمارات العربية المتحدة
PO Box 898, Abu Dhabi, UAE
adnoc.ae

شركة بترول أبوظبي الوطنية
Abu Dhabi National Oil Company

BUSINESS & COMMERCIAL SUPPORT DIRECTORATE

CUSTODIAN	B&CS/Group Information Technology Function/IT Security Risk & Compliance
DISTRIBUTION	All ADNOC Users

REVISION HISTORY

DATE	REV. NO.	PREPARED BY (Designation /Initial)	DESCRIPTION OF CHANGE
27 Oct 2019	0	Milen Nikolov, Sr. Analyst, Group IT Security Risk & Compliance Section	Initial draft based on the contents of the ADNOC Information Security Management System Standard.

1. DEFINED TERMS

"ADNOC" means Abu Dhabi National Oil Company.

"ADNOC Group IT Function" means ADNOC Group Information Technology Function within the B&CS Directorate**.**

"ADNOC Personnel" means ADNOC staff (together or individually), including officers, employees, contracted, temporary or seconded staff, or those that are on an internship.

"Asset" is anything that has value to the organization such as software, equipment, information systems.

"Availability" means the ability to timely and reliably access and use information assets.

"B&CS Directorate" means the Business & Commercial Support Directorate of ADNOC.

"BYOD", or bring your own device, refers to the practice where employees are allowed (or sometimes encouraged) to use their own personal devices to access selected non-public corporate information assets or specific enterprise services.

"CEO" means Chief Executive Officer.

"Confidentiality" means preserving authorized restrictions on information access and disclosure, including means for protecting personal and proprietary information.

"Corporate network" means the interconnected group of internal servers, systems, communications or computing devices that provide access for ADNOC Personnel to non-public ADNOC information services, and are owned, operated, or otherwise managed by the ADNOC Group IT Function.

"Data" is raw, unstructured and unorganized values that are not yet processed. Information is derived from data.

"HC&A Directorate" means the Human Capital & Administration Directorate of ADNOC.

"Information" is the contextualized representation of knowledge via facts, measurements, or data that is organized, retrieved, reproduced, stored, or communicated.

"Information Asset" means a body of knowledge or information resources (electronic or non-electronic) that ADNOC must have to conduct its business.

"Information Asset Custodian (IAC)" is an individual (or a group of individuals) to whom custody of an information asset has been delegated. The custodian with his respective subordinates and team members are responsible for the daily operations and management of the information asset and its associated controls, in line with the requirements, directions and instructions of the Information Asset Owner.

"Information Asset Owner (IAO)" is an individual (or a group of individuals) that manages or is responsible for a business function, which an information asset is serving or is directly associated with. The asset owner has administrative authority over the information asset, and is authorized to make decisions related to the asset's management throughout its lifecycle.

"Information Security Incident" is an occurrence that may negatively affect the confidentiality, integrity, or availability of an information asset, or constitutes a violation or imminent threat of violation of security policies or procedures.

"Information System" is an organized collection of resources for the electronic collection, processing, storage, and communication of information.

"IP" means Internet Protocol.

"Need-to-Know" is a principle where users are provided with a minimum set of information or system access rights or privileges, which are necessary to fulfil their job roles and responsibilities.

"Network device" means devices or equipment designed to facilitate the electronic communication of information.

"Non-repudiation" refers to assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

"Risk" is a combination of the probability of an adverse event occurring and its consequences.

"Risk Acceptance" is the decision to accept a risk.

"Risk Assessment" is the overall process of risk analysis and risk evaluation, including the systematic use of information to identify sources of, quantify or otherwise estimate the level of risk

"Risk Treatment" is the process of modifying a risk by implementing controls or measures that typically reduce its probability or impact.

"SVP" means Senior Vice President.

"Threat" refers to entities that may cause an information security incident, resulting in damages to the organization's information assets or reputation.

"UAE" means United Arab Emirates**.**

"Users" in the context of this document are ADNOC employees, contractors and third party personnel with access to organization's information, systems, or information processing facilities.

"VP" means Vice President.

"Vulnerability" is a weakness associated with an information asset (or a group of assets) that can be exploited by a threat to gain unauthorized access, make illegal modifications, or for other malicious purpose.

2. INTRODUCTION

2.1 This declaration captures the user's acceptance of all ADNOC terms related to the acceptable use of its non-public IT systems and services, including but not limited to the terms and conditions when accessing ADNOC Group IT Function-managed or controlled infrastructure, communications and collaboration services, computing devices and information systems.

2.2 All users that access or otherwise use non-public ADNOC Group IT Function-managed or controlled services or systems, or work within ADNOC premises, must read and accept these terms and conditions, and comply with their provisions.

3. SCOPE

3.1 All individuals accessing or using ADNOC non-public facilities, information assets or services, must be aware of the responsibilities and security requirements related to the usage of ADNOC information assets, and must place all reasonable efforts towards minimizing the organization's exposure to cybersecurity risks, including malware infections, loss or compromise of sensitive data, service disruption or legal issues.

3.2 You must become aware of, and comply with the provisions of the applicable ADNOC policies, standards, ancillary or supporting manuals and procedures, as well as all applicable laws.

3.3 The ADNOC Group IT Function may define and publish ancillary or subordinate manuals, guidelines and procedures to support the implementation of the relevant ADNOC policies and standards.

4. OWNERSHIP, REVIEWS & MAINTENANCE

4.1 The ADNOC Group Information Technology Function is the owner of the contents of this declaration, and responsible for its custody, maintenance, and periodic updates. The related standards will be reviewed and communicated at least annually to ensure its continuing suitability under the information security framework and in meeting the organization's compliance obligations and legal responsibilities.

5. ENFORCEMENT & EXEMPTIONS

5.1 Violations of ADNOC policies or standards will be subject to actions in accordance with the applicable laws and regulations, contracts and agreements, ADNOC Human Capital & Administration policies. Actions may range from verbal warning or revoked access to ADNOC facilities or services, to termination of employment/contract/agreement, or legal claims.

5.2 Exceptions or exclusions to this declaration or its related standards, may be granted based on the outcome of a cybersecurity risk assessment, endorsed by Group IT Function Senior Vice President, and residual risk accepted by the Information Asset Owner.

6. GENERAL PROVISIONS

6.1 Protect the ADNOC information assets that you own, or are in your custody.

6.2 When transacting, processing or using ADNOC information assets, use only devices, software, information systems and services that are authorized by the ADNOC Group IT Function.

6.3 ADNOC information assets and services must be used only for business purposes, unless explicitly stated otherwise (via the terms of use associated with a service, exemptions, or other appropriate means).

6.4 Never engage in activities that could be considered illegal, or may put ADNOC at risk. This includes (but is not limited to):

(a) Attempting to gain unauthorized access to communications, information assets, or systems;

(b) Impersonating others;

(c) Exposing confidential information to unauthorized parties;

(d) Performing unauthorized network or vulnerability scanning;

(e) Attempting to bypass information security controls;

(f) Exploiting software vulnerabilities;

(g) Interfering with the normal operation of information systems and services;

(h) Violating intellectual property rights.

6.5 ADNOC is committed to respecting the rights of its Personnel, including reasonable expectation of privacy. However, you are responsible for your activities while using the organization's information assets and services.

6.6 To maintain and ensure the security of information assets, and for legal and compliance purposes, with or without notice, the Group IT Function may:

(a) Record and monitor activities on ADNOC information systems, services and networks;

(b) Take actions towards protecting the confidentiality, integrity and availability of ADNOC information assets, including (but not limited to) denying or ceasing access to information systems, networks or services, taking control or custody of information assets and devices, collecting and preserving evidence, or other necessary lawful measures;

6.7 As part of official investigations, the Group IT Function may provide monitoring logs of activities or other related information to:

(a) Formal ADNOC ethics, disciplinary or audit committees involving the functions under the ADNOC Human Capital & Administration Directorate, the ADNOC Legal, Governance & Compliance Function, and/or the ADNOC Audit & Assurance Function;

(b) Authorized law enforcement representatives and competent government authorities.

6.8 Be familiar and comply with the other relevant ADNOC policies, standards, manuals and procedures while using the organization's information systems or services.

7. ASSET MANAGEMENT

7.1 ADNOC information assets must be classified, labelled and handled in accordance with the applicable policies, standards, manuals and procedures.

7.2 All information assets in custody must be returned to ADNOC before the end of employment or contractual obligations. This includes (but is not limited to) ADNOC or vendor documentation, devices, equipment, software licenses, or materials subject to intellectual property or copyright.

7.3 Before sharing with third parties information classified as "Need-to-Know" and above, make sure that:

(a) The appropriate legal and compliance requirements are met, including a valid Non-Disclosure Agreement (or a compliant legal contract);

(b) A cybersecurity risk assessment is conducted by the Group IT Function, and the identified cybersecurity risks are communicated with the Information Asset Owner and treated;

(c) You have the approval of the Information Asset Owner.

8. USER ACCOUNTS AND PASSWORDS

8.1 Never share your login credentials. Do not use login credentials or accounts belonging to others.

8.2 User accounts inactive for more than ninety (90) days will be disabled.

8.3 Change your account password as soon as you suspect it has been disclosed.

8.4 Passwords must not be stored or communicated in clear text or unencrypted.

8.5 Passwords must not be reused across services. ADNOC and non-ADNOC accounts must always use different passwords.

8.6 Use strong passwords that are not based on easily guessed keyword combinations that include company name, department or project name, personal or family members' details, trivial keyboard positions, etc.

9. NETWORK AND INTERNET SECURITY

9.1 Only devices authorized by the ADNOC Group IT Function may access or connect to the corporate network.

9.2 Personal or non-ADNOC devices may be connected to the designated visitor, employee, or meeting room wireless (Wi-Fi) networks.

9.3 Access to unauthorized websites and services will be blocked. The ability to connect to a website or use a service does not mean it is authorized.

9.4 Contact IT Service Desk to establish if a website or an online service has been approved for transacting ADNOC information.

9.5 ADNOC information must never be shared with unauthorized parties.

9.6 Users must never issue statements that may negatively affect the ADNOC's interests or reputation.

10. COMMUNICATIONS

10.1 ADNOC email messages or information must never be forwarded to personal email accounts.

10.2 Only approved email signatures and disclaimers may be used.

10.3 All communications must be consistent with the religious, cultural, political and moral values of UAE.

10.4 Never exchange messages containing:

(a) Defamatory, racist, obscene or otherwise offensive remarks; or

(b) Malicious attachments, links to malicious or illegal content.

10.5 Do not use email Blind Carbon Copy (BCC).

10.6 Suspicious email messages must be reported, including phishing attempts, fraudulent messages, malicious attachments or links, or other content that may be in violation of ADNOC policies or standards. These incidents may be reported via the dedicated phishing reporting button in the ADNOC email clients.

11. THIRD PARTY SOFTWARE AND SERVICES

11.1 Only software that is authorized by the ADNOC Group IT Function must be used.

11.2 Users must comply with the terms of the software licensing and usage agreement.

11.3 Authorization to use software and its installation may be requested via the IT Self Service Portal.

12. WORKSPACE SECURITY

12.1 Work or personal devices must be locked when unattended;

12.2 Users must log out from their sessions when leaving their office for more than a day.

12.3 Before leaving a meeting room, always erase any information written on white boards, remove or shred flip charts, and check for forgotten documents or equipment.

12.4 When printing or scanning documents, printouts or originals must be collected, and users must log out from any authenticated sessions with the printer/scanner.

12.5 Documents and devices containing sensitive or confidential ADNOC information must never be left unprotected. Users must:

(a) Shred drafts and unwanted copies of documents;

(b) Use locked cabinets to store devices and documents containing ADNOC confidential or sensitive information;

(c) Never leave personal or corporate electronic devices or documents unattended in public areas, such as meeting rooms, lobbies, reception areas.

13. DEVICES AND EQUIPMENT

13.1 Only ADNOC Group IT Function-authorized personnel may change the system configuration of ADNOC IT devices or equipment, or carry out relocation, maintenance, servicing, or otherwise perform technical support operations.

13.2 Fill the IT equipment movement form and obtain approval from the ADNOC Group IT Function when IT equipment needs to be moved into, within or out of company's premises.

13.3 Immediately report information security incidents involving the loss, theft, or damage of ADNOC IT assets or personal devices that may contain sensitive or confidential ADNOC information.

13.4 Do not use unauthorized removable media to transfer sensitive or confidential ADNOC information.

13.5 Always store important or business critical documents and information assets on ADNOC Group IT Function-provided content management systems, information systems, or network storage.

13.6 Never use endpoints (laptops, desktops, tablets) as the sole repository for storing important or business critical documents or data.

13.7 Use devices belonging to (or allocated to) others only with the Information Asset Owner's permission.

14. PHYSICAL SECURITY

14.1 Wear your ADNOC identity card visibly while inside the organization's premises.

14.2 Never leave identity cards unattended, or lend them to anyone.

14.3 Do not tamper with or duplicate identity cards.

14.4 The loss or theft of an identity card must be immediately reported to the reception desk, or to the Corporate Security Department.

14.5 Prevent tailgating attempts and inform the nearest security guard if you witness such an attempt.

14.6 Visitors or third parties must be escorted inside ADNOC premises by ADNOC Personnel to and from the specifically designated no-escort areas (receptions, lobbies, or other common locations explicitly designated as no-escort areas).

15. INFORMATION SECURITY INCIDENTS

15.1 Immediately report suspected information security incidents. Information security incidents may include, but are not limited to:

(a) Suspicious or non-compliant email messages, websites, or content;

(b) Fraudulent or suspicious activity that involves ADNOC information assets, systems or services;

(c) Malware infections;

(d) Lost, stolen, or abandoned devices;

(e) Unauthorized access to ADNOC information assets, systems or premises;

(f) Other violations of ADNOC policies, standards or manuals that may expose the organization to cybersecurity risks.

15.2 Information security incidents may be reported via:

(a) The IT Self Service Portal;

(b) Telephone to the IT Service Desk.

16. USER ACCEPTANCE

I acknowledge that I have received and read the above terms. I understand that it is my responsibility to comply with these and other relevant information security requirements that may be presented to me as part of my work at ADNOC.

Name: _____

Job Title: _____

Organization, Function/Division/Department: _____

Signature: _____ **Date:** _____/_____/_____