DUBAI
HOLDING

Employee Information Security Code of Practice

For the Good of Tomorrow

Table of Contents

1 Document Release Information

1.1 Document Control

File Name	Dubai Holding Employee Information Security Code of Practice v1.1.doc
Description	This document defines DH employee Information Security Code of Practice
Document Owner	Dubai Holding Information security
Version:	1.1
Status:	Final
Publish Date:	17 March 2019
Date of Next Review	17 March 2020
Applicable to:	Dubai Holding and its subsidiaries

2 Dubai Holding Employee Information Security Code of Practice

2.1 Introduction

Dubai Holding and its business units ("the Group") provide IT equipment's (such as laptops, tablets etc.) to allow employees (this includes any contractors, temporary staff and service providers) to access the necessary information to carry out their jobs.

The guidance of DH Employee Information Security Code of Practice helps and addresses several Information Security issues:

- Safeguarding the information that we use in all aspects of our business operations. This includes paper, computer files, emails, telephone conversations, faxes, instant messages used in DH systems and any other forms in which information is stored, transmitted or processed;
- Defending the Group from potential liabilities from unauthorized activity, e.g., theft of policy holder information, downloading of copyright or illegal material, implied contracts in email.
- Shielding staff information's and systems from external threats and preventing un-authorized access.

In order to maintain confidentiality, integrity and availability of information and for continuous success of our organization, it is our responsibility of each employee to protect our business and personal information.

2.2 Compliance

In using IT equipment (such as laptop's, tablets etc.) and to access any Group information, staff must follow the conditions set out in this Information Security Code of Practice. Employees are required to read and acknowledge the contents of this Code of Practice on joining the Group or signing any form of contract to work for the Group.

Please speak to Information Security team for advice on any aspects of this code.

2.3 The Code of Practice

2.3.1 Permitted Use

- Group equipment and resources are provided for business purposes; although limited personal use is permitted. All information processed or stored on Group equipment is viewed as a Group asset.

2.3.2 Prohibited Activities

The following list of actions shall be prohibited for the protection of information resources unless the activity is part of the employee's official job duty or is protected by local law:

- Installing any software or hardware on systems without prior approval and assistance of the appropriate technical support team.
- Using own applications in order to process "restricted" or "confidential" company information.
- Modifying or tampering with hardware or software provided by Dubai Holding and its subsidiaries.
- Camera in the building should be used with the management as well as security approval.
- Employees and third parties shall not use unapproved, cloud-based file synchronisation services or other unapproved cloud services and only IT Security approved cloud-based synchronization services shall be used.

- Providing restricted & confidential information about Dubai Holding and its subsidiaries to external parties is prohibited.

Note: this is not an exclusive list and the Group reserves the right to add to this list at any time when it is required by regulatory requirements and communicate changes to staff as necessary.

2.3.3 Access – General

- Access to systems, buildings and information should be authorised by line management and/or the information owner.
- Never attempt to exceed the authority levels granted to you.

2.3.4 Computer Systems & Devices Usage

- Computer systems, facilities and information provided by or on behalf of Dubai Holding and its subsidiaries in the course of its business operations or created by employees and third parties in the course of their employment, remain the property of Dubai Holding and its subsidiaries even after the employee resigned or left.
- To ensure the availability of the data, infrastructure and applications, employees and third parties shall use IT systems for business purposes only however some limited personal usage is allowed (browsing, research, news, business & economy, government services etc.).
- Employees and third parties are responsible for proper safekeeping and use of the computers and devices provided by Dubai Holding and its subsidiaries.
- Employees and third parties are required to promptly notify of any theft, damage or loss, as well as any malfunctions of IT systems (such as laptops, tablets etc..) which could affect the normal operation of the devices they use in their daily operations.
- Employees and third parties shall be vigilant of malware related threats and shall contact IT immediately if they suspect any malicious activity on their computers or any infection.
- Employees and third parties shall acknowledge their responsibilities in terms of protecting "restricted" or "confidential" data.

2.3.5 Clear Desk, Data Confidentiality & Privacy

- Employees and third parties shall follow physical security procedures including signing in all visitors and escorting visitors where necessary.
- Employees and third parties shall not leave information resources unsecured or unattended inside and outside Dubai Holding and its subsidiaries facilities.
- Employees and third parties shall retrieve all hard copy printouts containing restricted and confidential company information, from printers and fax machines as soon as they know the documents are available for pick up.
- Working areas shall be cleared of all physical information at the end of the working day.
- Access to removable media (USB, external hard disk) should be used by authorized individuals with proper approvals
- Documents shall be disposed of appropriately, including shredding where necessary.

2.3.6 Copyright & Intellectual Property Rights

- Employees and third parties shall adhere to intellectual property rights associated with information systems (Software licenses, copyright requirements) wherever applicable.
- All products (trademarks, industrial property, designs, copyrights etc..) related to Dubai Holding and its subsidiaries, created during employment are considered as Intellectual Property of Dubai Holding and its subsidiaries.
- All licensed material (software, images etc.) must only be used in line with the copyright conditions attached to them with proper approvals.

2.3.7 Use of Email & Instant Messaging Service

You are personally responsible for any email or instant messaging which you send. Consider the sensitivity and content of any messages you send and take appropriate measures to ensure that messages are sent securely and that the content will have no adverse impact on the Group.

- Email accounts shall be provided to employees and third parties for business purposes only.
- Email and attachments shall not contain content consisting of pornography, ethnic slurs, racial epithets, or anything that may be interpreted as offensive or with intent to harass others based on an individual's religion, sex, race, national origin or other characteristics.
- Employees and third parties shall use prudent judgment when composing messages and file attachments. The following shall be prohibited:
    1. For personal profit activities not sanctioned by the business
    2. Transfer of pornographic content
    3. Propagation of chain letters
    4. Harassment of any kind
    5. Mass-mailings or spamming
    6. Compromising the privacy of employees or confidentiality of data
- Users shall not open any link or attachment received in emails unless they verify it is a legitimate email from a known sender if it doubts please report it immediately to IT Service Desk for further analysis.
- The use of personal email accounts for Dubai Holding and its subsidiaries business activities shall be prohibited.

2.3.8 Internet and Social Media Usage

- Employees and third parties shall not access websites in order to perpetrate behavior that is inappropriate, unless required in their normal course of duties. Such behavior includes:
    1. Accessing pornography or other sexually explicit material.
    2. Accessing sites comprising of hate speech or other potentially violent or criminal activity.
    3. Committing piracy or copyright infringement.
    4. Using the Internet to send offensive or harassing material to others.
    5. Downloading software or any copyrighted materials unless covered or permitted under an appropriate agreement or license benefiting Dubai Holding and its subsidiaries.
    6. Malicious activity such as network port scanning unless explicitly permitted.
    7. Publishing defamatory or knowingly false material about anyone including Dubai Holding and its subsidiaries, its staff, its customers or its business partners.
    8. Revealing confidential information about Dubai Holding and its subsidiaries, its business practices and ventures, its staff, its customers or its business partners.
    9. Undertaking activities that will subvert IT team effort or network resources.
    10. Deliberately attempting to introduce any form of malicious software into the corporate network.
- Employees and third parties must not use their Dubai Holding and its subsidiaries identity information, logon IDs and passwords when using Internet sites and social networking sites for their personal use.
- When using any public platform where the employee is identified as Dubai Holding or its subsidiaries, the employee shall:

1. Clarify that what is expressed indicates an opinion of the employee and not an official statement of Dubai Holding and its subsidiaries where relevant.
2. Observe the requirements regarding confidentiality, privacy, acceptable use and intellectual property.

2.3.9 Monitoring & Enforcement

- The use of Dubai Holding and its subsidiaries systems and devices is being monitored and logged in order to comply with any legal obligations or regulatory & business requirements.
- Violations of the information security policies shall be subject to investigation and remediation which may include disciplinary action.

2.3.10 Remote Working

- Employee shall use IT approved VPN facility while connecting to DH network remotely from public places, meeting rooms and other unprotected areas.

2.3.11 Report Incidents and Violations

- All employees and third parties shall be required to note and report any observed or suspected incidents, violations, security weaknesses and malfunctions in systems or services.
- Employees and third parties shall co-operate fully, and to the best of their ability, if requested to assist in the investigation of a security incident.
- Employees and third parties shall not discuss, details of actual or suspected security incidents without proper approvals.

2.4 Agreement

All Group staff are required to complete and sign this agreement by signing this document.

I have read and understand the Dubai Holding Information Security Code of Practice and accept that all access and activity, as well as data is subject to monitoring" and I will comply with the requirements specified in this document.

Name: SUMIT MAHESHWARI

Signature: Sumit

Date: 07-02-2024

Sumit