Information Technology

Usage Policy

This Information Technology Usage Policy has been approved by the CEO of Ittihad International Investment LLC

……

P.O. Box 41188, Abu Dhabi, UAE. Tel: 026581888, FAX: 026581800

Table of Contents

Introduction

Information Technology (IT) systems and networks are an integral part of business at Ittihad International Investment LLC and subsidiaries – henceforth the "**Company**". The Company provides computer devices, networks, and other electronic information systems ("**Systems**") to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets.

This Policy and directives (the "Policy") have been established in order to:

- Establish responsibilities and guidelines for usage of IT resources and services.
- Establish acceptable and unacceptable use of IT resouces and services.
- Safeguard the information contained within these systems.
- Reduce business and legal risk, and protect the good name of the Company.

Scope

This IT Usage Policy applies to all employees of the Company who have access to or, where applicable, temporary possession of the Systems to be used in the performance of their work.

Administration

The IT Manager as head of the IT Department is responsible for the administration of this Policy. The designated review committee is responsible to approve this Policy.

The Company's IT Usage Policy, as explained in this manual, does not purport to be comprehensive and may be changed from time to time as business conditions dictate or require. If and when provisions are changed,you will be informed as soon as practicable.

The Company, at its option, may change, delete, suspend or discontinue any part or parts of the Policy in this manual at any time without prior notice. Any such action shall apply to existing as well as future employees.

1. Statement of responsibility

General responsibilities pertaining to this Policy are set forth within the overall IT Usage Policy. This section lists additional specific responsibilities.

1.1 Line Manager responsibilities

Line Managers will ensure that all appropriate personnel are aware of and comply with this Policy, and any amendments thereof.

1.2 IT Department responsibilities

The IT Department will:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these Policy directives.
- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this Policy directive.

2. Acceptable Usage: Software and Hardware

This section defines the boundaries for the "acceptable use" of the Company's electronic resources, including software, hardware devices, and network systems.

Hardware devices, software programs, and network systems purchased and provided by the Company shall normally be used only for creating, researching, and processing Company-related materials. By using the Company's hardware, software, and network systems you assume personal responsibility for their appropriate use and agree to comply with this Policy and other applicable Company policies, as well as local emirate and UAE federal laws and regulations.

2.1 Software and Hardware

All software and/or hardware devices acquired for or on behalf of the Company or developed by Company employees or contract personnel on behalf of the Company is and shall be deemed Company property. All such software and/or hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

2.1.1 Purchasing

All purchasing of Company software and/or hardware devices must be approved by and centralized through the IT department to ensure that all applications conform to corporate standards and are purchased at the best possible price and highest warranty. All requests for corporate software and/or hardware devices must be submitted to the line manager of the relevant department for approval. The request must then be sent to the IT department, which may then determine – without any obligations - the standard solution that best accommodates the desired request.

2.1.2 Copyrights and license agreements

It is the Company's Policy to comply with all legal obligations regarding intellectual property.

The Company and its employees are legally bound to comply with all applicable UAE laws, decrees, regulations and orders related to Intellectual Property rights ("**Laws**"), as well as all proprietary software license agreements. Noncompliance can expose the Company and the responsible employee(s) to civil and/or criminal penalties. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be in violation of the Laws. In addition to violating such Laws, unauthorized duplication of software is a violation of the Company's IT Policy.

2.1.3 IT Department responsibilities

The IT Department will:

- Maintain records of software and hardware device licenses owned by the Company.
- Periodically scan corporate network to verify that only authorized software and hardware devices is installed.

2.1.4 Employee responsibilities

Employees shall not:

- Install any software and/or hardware devices unless authorized by IT department. Only software and/or hardware devices that is licensed to or owned by the Company is to be installed on the Company's Systems subject to the approval of the IT department.
- Copy software unless authorized by IT.
- Download software unless authorized by IT.

3. The Internet and e-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide.

3.1 Policy

Use of the Internet by employees of the Company is permitted and encouraged where such use supports and enhances the goals of the business. Access to the Internet is a privilege and all employees must strictly adhere to the Company's policies. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also filled with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the Company's interests, the following guidelines have been established for using the Internet and e-mail.

3.2 Acceptable usage

Employees using the Internet are representing the Company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites.
- Using e-mail for business correspondence.

3.3 Unacceptable usage

Employees must not use the Internet for purposes that are illegal, unethical, nonproductive, or harmful to the Company as may be decided by the Company at its sole discretion from time to time. Some examples of such unacceptable usage are, but not limited to:

- Conducting any personal business using Company resources or Systems.
- Illigetimate gain that are attributable to the copy right infrengment
- Transmitting any content that is offensive, harassing, or fraudulent using the Internet or the Company's email service
- Using the Systems to conduct any act of fraud, and/or software, film or music piracy.
- Downloading files not related to work and especially copying or pirating software and electronic files that are copyrighted, without authorization.
- Sharing confidential material, trade secrets or proprietary information outside of the Company.
- Sending or posting information that is defamatory to the Company, its products/services colleagues and or clients.
- Using Company's e-mail or IP address to engage in conduct that violates Company's policies or guidelines
- Passing off personal views as representing those of the Company.
- Access to sites that contain obscene, hateful, pornographic, unlawful, violent, illegal or otherwise culturally insensitive material as deemed by the Company.

3.4 Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

- Ensure that all communications are for professional reasons and if not, that they do not interfere with his/her productivity.
- Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
- Not transmit copyrighted materials without permission.
- Run a virus scan on any executable file(s) received through the Internet.

3.5 Employee email and computer data privacy

All messages created, sent, or retrieved over the Internet are the property of the Company.

In some cases, Ittihad International Investment LLC ("**III**") may be required to audit or access the computer data of any of the Company's employees. In such instances III will endeavor to seek the consent of the employee. If this is not possible for whatever reason (i.e. in the absence of the employee, or if there is an ongoing investigation, etc…), approval to audit or access an employee's computer data shall be referred to a committee who shall have final authority on whether or not approval is granted. The committee will be made up of III's CEO, III's CFO, III's General Counsel and III's HR Manager and approval to audit or access the employee's computer data shall be deemed to have been granted upon the consent of at least two members of the committee – inclusive of the III's CEO.

In cases where a subsidiary of III wishes to audit or access its employee's computer data, then the conditions of the preceding paragraph will apply insofar that approval to audit or access an employee's account shall be granted upon the consent of the subsidiary General Manager and at least any one member from the aforementioned committee.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver as part of an ongoing investigation in line with the Company's policies

4. Computer viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

4.1 Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

4.2 IT Department responsibilities

IT Department shall:

- Install and maintain appropriate antivirus software on all computers and Internet access points.
- Respond to all virus attacks and destroy any virus detected.

4.3 Employee responsibilities

These directives apply to all employees:

- Employees shall not knowingly introduce a computer virus into Company computers and network.
- Employees shall not introduce to the Company computers any media devices (ex. CDs) of unknown origin.
- No outside equipment maybe plugged into the corporate network without approval from the IT department (ex. vendor laptops)
- Incoming media devices shall be scanned for viruses before they are read.
- Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY UNPLUG THE NETWORK CONNECTION OR POWER DOWN the workstation and call the Help Desk or any IT department personnel.

5. Wireless Access Policy

The goal of this Policy is to protect the IT resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to our public image.

All users employing wireless methods of accessing corporate technology resources must adhere to Company-defined processes for doing so, using Company-approved access points.

5.1 IT Department responsibilities

- All wireless access points connecting to the corporate network must be approved by Ittihad International Investment LLC's IT department.
- The IT Deparment reserves the right to turn off without notice any access point connected to the network that it feels puts the Company's systems, data, users, and clients at risk.

5.2 Employee responsibilities

- Use of the wireless network is subject to the same guidelines as the Company's technology, Internet, and email acceptable use policies.
- Access to the corporate and/or guest wireless network must be approved by the IT department. Acess to the corporate and/or guest wireless network must adhere to the corporate policies and standards.
- The wireless access user agrees to immediately report to his/her manager and/or IT Department any incident or suspected incidents of unauthorized access point installation and/or disclosure of Company resoursces, data, networks, and any other related components of the organization's technology infrastructure.

6. Access codes and passwords

The confidentiality and integrity of data stored on Company computer systems must be protected by access controls to ensure that only authorized employees have access.

6.1 Policy

Any employee requesting authorization to any software must have his/her line manager request for such approvals either through filling the appropriate form or by sending an email.

Similarly, deletion and modification of user access controls must be requested by the employees' line manager. It is the responsibility of the department head to ensure that access control granted to their staff are periodically reviewed to conform to their current responsibilities.

6.2 IT Department responsibilities

The IT Department shall be responsible for the administration of access controls to all Company computer systems. The designated IT personnel will process additions, deletions, and changes upon receipt of a formal request from the end user's supervisor.

6.3 Employee responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall not steal, use or disclose someone else's password.
- Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.

- shall change his/her passwords at least every 90 days (or as requested automatically using System Policies).
- Should use passwords that will not be easily guessed by others.
- Should lock or log out when leaving a workstation for an extended period.
- Should report, to the IT department, if he/she have access to data that is not needed to perform their job.

6.4 Line manager's responsibility

Line managers should notify in advance the IT Department whenever an employee is going to leave the Company or going to transfer to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

7. Physical security

It is Company Policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

7.1 Employee responsibilities

- All files on local workstation hard drives are considered transient, and are not backed up to tape. Therefore, ensure that all data are on the server (either in user's home folder or shared network drives).
- Any storage media devices (ex. CDs, usb key, etc) should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
- Any storage media devices should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
- Employees shall not take shared portable equipment such as laptop computers out of the office premises without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
- Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

8. Outsourcing

This is to maintain the security of information when the responsibility for information processing has been outsourced to another organization

8.1 The Policy

Outsourcing arrangements must be governed by a formal contract that stipulates the security requirements as necessitated by the type of work performed and the criticality of the data at the outsourcing location.

All outsourced IT related projects or work must be approved by and centralized through the IT department of Ittihad International Investment LLC.

9. Domain Name Registration Policy

This Policy applies to the Company. This Policy provides requirements for how the Company can obtain and safeguard certain internet domain names by establishing naming requirements, and a central registration and tracking process.

Any request for the creation or usage of domain name must be submitted to the IT Department of Ittihad International Investment LLC for approval and registration.

10. Website and Email Policy

This Policy has been developed in order to streamline Website and Email management, content submission, and posting process.

10.1 The Policy

- All and any requests for Website and Email hosting selection shall be reviewed by the IT department of Ittihad International Investment LLC which may then determine, – under its own discretion, the standard solution that best accommodates the desired request.
- Website and Email management and maintenance will be conducted by the IT department of Ittihad International Investment LLC.
- All Website content submissions must be sent to the IT department of Ittihad International Investment LLC. All requests will be channeled to the right approval authority.

11. Guidelines for requesting IT services

This Policy is to formalize procedure for the Company's employees to request assistance from IT.

11.1 Requesting IT support

The following methods can be used to contact the IT helpdesk:

- Contact the IT helpdesk by intiating a support ticket. Support ticket can be initiated by sending an email to the following email **……@ittihadinvestment.ae**
- Contact the IT helpdesk using the following email **……@ittihadinvestment.ae**
- Contact your assigned IT personel at your site.

12. Enforcement

Failure to observe these guidelines may result in disciplinary action (whether in the form of a warning, fine, claim for damages, termination or otherwise in accordance with the Company's Employment Manual) as determined in the Company's sole discretion and in accordance with Company Policy depending upon the nature and severity of the violation, whether it causes any liability or loss to the Company, and/or whether there exists a pattern of any repeated violation(s). The enforcement of this Policy and any disciplinary action brought as per the Company's Policy shall be without prejudice to any rights or remedies available to the Company under Federal Decree Law No. 5/2012 on Combating Cyber Crimes, Federal Law No. 37/1992 Concerning Trademarks, Federal Law No. 7/2002 on Copyrights and Related Rights and any other applicable UAE laws..

12.1 Civil penalties

Violations of any of the laws mentioned herein may expose the concerned legal entity and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Fines
- Confiscation of equipment

12.2 Criminal penalties

Violations of any of the laws mentioned herein that are committed “willfully and for purposes of commercial advantage or private financial gain” may expose the concerned legal entity and the employee(s) responsible to the following criminal penalties:

- Fines
- Jail terms

Acknowledgment of Information Technology Usage Policy

This form is used to acknowledge receipt of, and compliance with, Information Technology usage Policy for Ittihad International Investment LLC and subsidiaries – henceforth "the Company".

Procedure

Complete the following steps:

1. Sign and date in the spaces provided below.
2. Return this page to your line manager or human resources.

Signature

By signing below, I agree to the following terms:

I. I have received and read a copy of the "Information Technology Usage Policy" and understand and agree to the same.

II. I undertake to keep myself aware and up to date with any changes to the "Information Technology Usage Policy" as notified to me from time to time by the Company.

III. I understand and agree that any software, hardware devices, and storage media provided to me by the Company contains proprietary and confidential information about the Company and its clients or its vendors, and that this is and remains the property of the Company at all times and I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at the Company), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software.

IV. I agree that, if I leave the Company for any reason, I shall immediately return to the Company the original and copies of any and all software, hardware devices, storage media that I may have received from the Company that is either in my possession or otherwise directly or indirectly under my control.

V. I understand and agree I must make reasonable efforts to protect all the Company-provided software, hardware devices, and storage media from theft and physical damage.

VI. I understand and agree I must make reasonable efforts to protect accuracy, integrity and availability of the Company's data.

Employee signature:_____

Employee name: _____

Date: _____

Department: _____

CompanyCompany_____