United Capital

United Capital Information Information Security Policies.

United Capital

COMPUTER USAGE POLICY AND GUIDELINES

1. 2.1 Introduction

Abuse or adverse use of computer infrastructure by authorized and unauthorized users could pose a very high security risk to the United Capital's entire infrastructure and critical assets.

This underscores the need to define acceptable systems use in line with the UC's established culture of openness, trust, and integrity. It is the corporate responsibility of all users (employees and associates) to ensure that the organization's system is not abused or used illegally either knowingly or unknowingly.

2. 2.2 Purpose

This Computer Usage Policy and Guidelines (the "Policy") sets to provide direction on the procurement, use, security, and disposal of official computers of members of staff of the United Capital Plc.

3. 2.3 Scope

This policy applies to employees, contractors, consultants, and others working at United Capital, including all personnel affiliated with third parties. This policy applies to all computers whether owned or leased by the organization.

2.4 Responsibility

The Information Technology Department and its leadership shall have responsibility for the deployment of and compliance with this policy subject to

Roles	Responsibilities
Information Technology	• The team shall be a custodian of this policy and responsible for ensuring that all its operations and procedure comply with the provisions of this policy, it can also propose amendments to this policy as may be required. • The team is responsible for the deployment, and compliance to the policy. • The Unit is responsible for carrying out quality control to verify that the specification of the computer devices procured meets the required specifications. • The Unit is responsible for the installation of applications and security tools to protect United Capital Group's data/information on new and existing devices. • The Unit is responsible for retrieving devices and cancelling associated services when an employee no longer requires the device or leaves the organisation. • The Unit shall carry out an assessment/diagnosis of the computer devices and advise Corporate Services on recommended actions in case of damages.
Corporate Services	The Unit is responsible for the procurement of all computer and technology devices e.g., Laptops, desktops, accessories etc. *(Ref. section 3.12)*
Internal Control	• Regularly carry out review of all computer systems/platforms. • IT Control Unit shall conduct periodic review of the employee's laptops and desktops inventory and is responsible for investigating any incidence of device loss with recommendation to the Management. *(Ref. 2.18.3)*
Information Security	• Responsible for the overall ownership and implementation of this policy. • Shall conduct necessary oversight where this policy is concerned and perform assurance functions to secure the United Capital environment.

1. 2.5 Definitions

2.5.1 In this Policy, the use of the term 'Computer' refers to devices such as Notebooks, Desktop computers and Laptop computers.

2.5.2 Computer is construed to include all its accessories, whether purchased along with the computer or at any time during its useful life.

2.6 Deployment of Desktops and Laptops

2.6.1 A desktop shall be provided to employees in the following instances:

2.6.1.1 Where an employee is not expected to work outside the office.

2.6.1.2 Where an employee will be handling data that is too sensitive to move off-site or remote locations.

2.6.1.3 Where the computer system is to act as a server.

2.6.1.4 Where the nature of the employee's job requires the use of a desktop.

2.6.2 All other employees shall be provided with laptop for official use.

2.6.3 Where an employee elects and is approved to use his/her private laptop for official duties, then such will be subjected to the use of personal laptops and BYOD policy provided in this policy handbook.

2.7 Laptops and Desktops Specifications

2.7.1 All Laptops and desktops to be purchased shall conform to the following specifications. Any other variation shall be approved by the Group CEO upon recommendation by the Heads of Information Technology and Information Security.

2.7.1 All workstations on the network shall have the approved latest version of Microsoft Windows Operation Systems installed. Minimum specifications for laptops and servers are Windows 10 OS and Window Server OS 2016 and above respectively.

2.7.2 Hand-held mouse and keyboard shall be provided to staff on request with proper justification for the duplication over mouse pads and keyboards and approval.

2.7.3 Laptop security cable lock shall be provided for the staff that are using laptops to ensure their laptops are locked down while away.

2.7.4 Laptop bag with protective sleeves shall be procured along with the purchase of new laptop.

2.8 Use of Personal Laptops

2.8.1 Employees who want to use their personal laptops on the UC's network will do so subject to approval by the Group Chief Information Security Officer.

2.8.2 Minimum Requirements

2.8.2.1.0 Any personal laptop shall be subjected to UC's information security checks which include but are not limited to:

2.8.2.1.1 Password protection

2.8.2.1.2 UC's Domain policy

2.8.2.1.3 Company antivirus, drive encryption and other endpoints security solution installation.

2.8.2.1.4 Approved latest operating systems for Windows laptops.

2.8.2.1.5 Data backup and synchronization with a file server, etc.

2.8.3 Authority

The employee must agree to provide unlimited authority over the laptop for the sole purpose of protecting UC's data and access on the laptop. This authority includes permission to wipe and debrief the laptop of company data in the event of loss or disposal. This may include personal data, address books and e-mail depending on the data classification of information locally stored.

2.8.4 Security

2.8.4.1 The employee shall be responsible that the personal laptop is adequately secured against loss, theft or use by persons not authorized by company policy to access company data to use the laptop.

2.8.4.2 The laptop must be locked down by the laptop security lock cable while away from the office.

2.8.4.3 All approved endpoint protections solutions must be installed to fortify the laptops/desktops against internal and external attack.

2.8.5 Support

The employee shall be responsible for replacing, maintaining, and arranging technical support for the personal laptop. UC will only provide

hardware, operating system or application support for the applications that have been installed by UC.

2.8.6 **Monitoring**

UC may monitor employee's use of the personal laptop while it is connected to UC's network. This information may be collected and archived.

2.8.7 **Software Licenses**

Employees shall abide by all license terms and conditions applicable to any software, apps, data, or information provided by UC to the personal laptop.

2.8.8 **Personal Data Backup**

Employees shall be responsible for backing up and restoring the data and configuration settings of their personal laptops. Personal data is not to be backed up or stored on UC network. The Organization will not be responsible for any personal loss, damage or any other liabilities that may occur because of actions undertaken by the employee to protect his/her data stored on the personal laptop.

2.8.9 **Resignation from the UC**

The Organization's data could be breached from personal laptop. Employees that use personal laptops shall submit such to the IT Department for reviews during the exit process from the company. These reviews may include manual checks for Company's data, removal and deletion of all Company data and application software installed. This process must be validated by the Information Security Department.

2.9 **Computer Resource Usage**

UC's computer resources, including servers, email, network, applications, laptops, and workstations provided to employees and contractors, are intended for official business use only. Occasional personal use is however acceptable with strict adherence to the UC's Information Security policy.

2.10 Computer Maintenance

2.10.1 To secure the computers and allow them to last long, the following principles shall guide their use and handling by employees.

2.10.1.1 Employees shall not carry laptops by their lids or screens as this would weaken the lid joints or crack them with time.

2.10.1.2 Employees shall not drop laptops with a thud as this could cause damage to the internal components.

2.10.1.3 While shutting down laptops and packing them, employees shall not slam their lids down with force as this could weaken their joints and crack the screens overtime.

2.10.1.4 Employees shall desist from haphazardly shoving the adapters (charger) into the power ports at weird angles or in similar ways that brings tension on the charger.

2.10.1.5 Employees shall disconnect their charger from electricity when not in use.

2.10.1.6 Employees shall keep their laptops away from all liquids and spills.

2.10.1.7 Employees shall tap their keyboards with care. Hard tapping would weaken them with time.

2.10.1.8 Employees shall ensure adequate ventilation for their laptops whenever the laptops are in use.

2.10.1.9 Employees shall ensure that their laptop is lockdown with laptop security lock while away.

2.10.1.10 Employees shall clean their laptops from time to time with a dry and clean napkin.

2.10.1.11 Approved Antivirus solution and other endpoint protection shall be installed on all employees' official laptops and desktop computers. This should be centralised, driven by IT Department, and monitored by IT Risk and Control.

2.10.1.12 Employees shall ensure that the official laptop is shutdown properly after daily usage, not just closing the lid. This is important for the installation of windows update to be completed.

2.10.1.13 Employees shall be responsible for the cost of repair in the event of physical damage to the laptop's component.

Except where established that the cause of the damage was not due to negligence.

2.10.1.14 In the event of damage laptop, IT department shall assess the laptop and advise the corporate services whether the cost of the repair should be paid by the employee or the business.

2.10.1.15 The actual amount to be paid shall be determined by the nature of damage. In some cases, employee may be asked to pay for complete replacement.

2.10.1.16 In the event of loss of official laptop, the incident shall be investigated by the Internal Control unit. The employee shall be responsible for the cost of replacement except where established the cause of lost was not due to negligence.

2.10.1.17 Employees should be security conscious and avoid displaying their laptop recklessly in the car or within their premises.

2.10.1.18 Employees should avoid moving around with the official laptop except when necessary.

2.10.1.19 Employees shall desist from all forms of negligence or act that could result into lost or theft of official laptops.

2.10.1.20 IT Control Unit shall conduct quarterly review of the employee's laptops and desktops inventory and present a report to management.

2.11 Computer Security

Employees have the ultimate responsibility for securing their official computers. The Information Security policy outlines detailed procedures for securing official computers and UC critical information.

2.12 Procurement

2.12.1 Procurement of computers shall be done by the Corporate Services Department in accordance with the processes outlined in the UC Procurement policy and as approved from time to time under the supervision of the UC Vendor Selection Committee (VSC).

2.12.2 Corporate Services Department shall adhere to the staff category list and ensure that laptops are procured based on the specifications approved for each of the categories.

2.12.3 Corporate Services Department shall ensure that laptops and other devices procured are onboarded into the Asset Inventory Management Application before releasing such devices to the users.

2.12.4 Corporate Services shall ensure that laptops are onboarded on the UC's Laptop insurance policy within a month of procurement.

2.13 Disposal

2.13.1 Laptops shall have a useful lifespan of three (3) years from purchase. Laptops which have exceeded their useful lifespan can be repurchased by the user at the net book value advised by the Finance Department.

2.13.2 Finance Department shall compute the laptop net book value using the depreciation method adopted for Computer assets in the organization.

2.13.3 Where a laptop becomes unusable before the stipulated 3-years period, the employee's supervisor shall inform IT Department for the system assessment. IT department shall make recommendation to Corporate Services for the replacement of the faulty laptop or otherwise. This recommendation should be approved by the Director of Digital Transformation.

2.13.4 Employees who resign after two years (24) months of allocation of laptops have the option to purchase their laptops at their net book value plus the 10% of the original cost price.

2.13.5 Right of first refusal is given to employees whose laptop has reached or exceeded the useful lifetime of three years.

2.13.6 Employees who take the top-up option, if exiting before the full depreciation of the laptop, shall be required to pay the net book value of the asset.

2.13.7 Ownership: Prior to the end of their useful life and until sold or auctioned as indicated above, computers remain the property of UC and all other conditions shall apply. Users may be asked to submit the laptop for routine maintenance or a physical count exercise.

2.13.8 Software and Data: All data on the laptop shall be backed-up to the shared drive and remove completely before a laptop is sold to the user.

2.13.9 The disposal of the obsolete Desktop Computer CPU and network devices should be done in accordance with the guidelines provided in the UC's Disposal of Obsolete Information Technology (IT) Equipment and Media Policy.

2.14 Bring Your Own Device (BYOD) Policy

UC grants its employees the privilege of purchasing and using smartphones and tablets of their choice at work for their convenience. UC reserves the right to revoke this privilege if users do not abide by the policies and procedure outlined below. This policy is intended to protect the security, confidentiality, integrity and availability of UC's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. UC employees must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network.

2.15 Acceptable Use

The Company defines acceptable business use as activities that directly or indirectly support business of UC.

2.15.1 Email and Communications Activities Acceptable Use Policy

2.15.1.1 The right to create/ delete UC staff on the Email System shall be approved by the Head, Human Resources.

2.15.1.2 Consultants and/or service providers requesting access into the email system shall be recommended by the Director of Digital Transformation and approved by the Group Chief Information Security Officer.

2.15.1.3 Creation of email work group shall be approved by the Internal Control Department.

2.15.1.4 Access to personal mailbox other than that of the authorized user shall be authorized by the Head of Internal Control.

2.15.1.5 The email forwarding must be approved by the employee Line Manager/supervisor before configured by IT Department.

2.15.1.6 The email forwarding configured must be stopped and the exited user account disable on the email platform after 1month of exit.

2.15.1.7 Increase in the email box size shall be authorized by the line Supervisor and approved by Head of Internal Control.

2.15.1.8 Authority to send mail to United Capital All Staff Group shall be authorized in line with Internal Communication Policy as approved by the Board of Directors.

2.15.1.9 Awareness campaign and/or sensitization memos shall be authorized by the Head of MCC.

2.15.1.10 The Group Chief Information Officer shall determine the appropriate size of the attachment to be allowed on the Group Email System subject to ratification by the ISC.

2.16 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., after appropriate authorization and documentation).

2.16.1 System and Network Activities Unacceptable Use

The following activities are strictly prohibited.

2.16.1.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UC is strictly prohibited.

2.16.1.2 Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the Company.

2.16.1.3 Devices may not be used at any time to:

i. Store or transmit illicit materials.
ii. Store or transmit proprietary information belonging to another company.
iii. Harass others.

2.16.1.4 Unauthorized copying of copyright materials including, but not limited to, digitization and distribution of photographs from magazines, books or other copyright sources, copyright music, and the installation of any copyright software for which UC or the end user does not have an active license is strictly prohibited.

2.16.1.5 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate authorities shall be consulted prior to export of any material that is in question.

2.16.1.6 Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is not allowed.

2.16.1.7 Revealing your account password to others or allowing use of your account by others is prohibited. This includes colleagues, family, and other household members when work is being done at home.

2.16.1.8 Using the organization computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction is prohibited.

2.16.1.9 Effecting security breaches or disruptions of network communication, Security breaches include, but are not limited to, accessing data for

which the employee is not an intended recipient or logging into a server or an account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but not limited to, network spoofing, packet sniffing, pinged floods, denial of service, and forged routing information for malicious purposes.

2.16.1.10 Port scanning or security scanning is expressly prohibited by any employee except for IT and Information Security with express approval of the Director of Digital Transformation and Group Chief Information Security Officer.

2.16.1.11 Executing any form of network monitoring which shall intercept data not intended for the employee's host unless this activity is part of the employee's normal job/duty.

2.16.1.12 Circumventing user authentication or security of any host, network or account is prohibited.

2.16.1.13 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack) is prohibited.

2.16.1.14 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet is not allowed.

2.16.1.15 Disabling of systems audit trail without express and written approval from Internal Control unit is prohibited. The audit trail or logging of all critical systems shall be enabled.

2.16.1.16 Removing/Uninstalling any of the approved endpoint protection solutions from official laptop/desktop without justification and approval by the Group Chief Information Security Officer.

2.16.2 Email and Communications Activities Unacceptable Use (Prohibition)

2.16.2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2.16.2.2 Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.

2.16.2.3 Unauthorized use, or forging, of email header information.

2.16.2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

2.16.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

2.16.2.6 Blind copy of staff or external party in the email correspondence.

2.16.2.7 Use of unsolicited email originating from within UC's networks, or service providers on behalf of the Organization to advertise, any service hosted by UC.

2.16.2.8 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.17 Devices and Support

2.17.1 Smartphones including iPhones, iPads, Android (all Android devices running on Android Nougat and above) and Blackberry phones (BlackBerry OS 10 and above) are allowed. Request to connect these devices to the UC network shall be based on business justification and approval of the DDT.

2.17.2 Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

2.17.3 Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

2.18 Loss/Stolen Devices

2.18.1 Lost or stolen devices must be reported to the Company within 24 hours via email. If it is an official laptop, such incident should be reported to employee Supervisor, Internal Control, Corporate Services, and IT Departments for appropriate steps to be taken to secure company data and information. Failure to report will render the custodian of such device liable for replacement of said laptop and possible further consequence for any breach of company data.

2.18.2 Employees are responsible for notifying their mobile carrier immediately upon loss of a mobile device or at worst within 24hours if the device contains UC's information or data.

2.18.3 Internal Control Unit is saddled with the responsibility to investigate any incidence of device loss and offer recommendation to the Management.

2.18.4 Staff will bear the cost of replacement of Company's asset where it is proven that the loss is due to negligence.

2.18.5 IT has responsibility for wiping company data off lost devices with the mobile device management tool upon approval by the Director of Digital Transformation and the Group Chief Information Security Officer.

2.19 Security

2.19.1 To prevent unauthorized access, devices must be password protected. A strong password is required to access the company network.

2.19.2 The Company's password policy is: Passwords on all systems must be at least eight characters and a combination of upper and lower-case letters, numbers and special character. Passwords will be rotated every 30 days for core business applications and 90days for the organization's active directory. The new password cannot be one of 10 previous passwords.

2.19.3 For the critical databases(Oracle and Postgre), Password complexity feature must be enabled. The minimum password length should be at least fifteen characters and a combination of at least one lower-case letters, numbers, and special character. The password age should be 90days. The new password cannot be one of 10 previous passwords. Password cannot contain part of user ID or the user ID itself.

2.19.4 Devices must be configured to auto lock with a password or PIN after being idle for five (5) minutes.

2.19.5 After five failed login attempts, the device will become locked and unlocked automatically after 30minutes for another login attempt.

2.19.6 Incident of account locked lock should be forward to the admin for password reset.

2.19.7 Employees are automatically prevented from downloading, installing, and using any app that does not appear on the Company's list of approved apps on official device.

2.19.8 Smartphones and tablets that are not on the Company's list of supported devices are not allowed to connect to the network.

2.19.9 Smartphones and tablets belonging to employees that are for personal use only can connect to the guest network only.

2.19.10 Employees' access to the company data is limited based on user profiles defined by Information Security/Internal Control and automatically enforced.

2.19.11 The employee's device may be remotely wiped off if 1) the device is lost, 2) the employee terminates his or her employment, 3) there is detection of a data or policy breach, a virus or similar threat to the security of the Company's data and technology infrastructure.

2.19.11 All personal laptops must be protected with an active and updated antivirus before they can be allowed on the UC network.

2.20 Risk/Liabilities/Disclaimers

2.20.1 While IT department will take every precaution to prevent the employee's personal data from being lost in the event it must remotely

wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

2.20.2 The Company reserves the right to disconnect devices or disable services without notification.

2.20.3 The employee is always expected to use his or her device in an ethical manner and adhere to the Company's acceptable use policy as outlined above.

2.20.4 The employee is personally liable for all costs associated with his or her device.

2.20.5 The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

2.20.6 The employee is mandated to read this policy and consent to its provision.

2.20.7 UC reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.

2.21 Waivers

The Group CEO shall approve all requests for any waiver to this Policy.

2.22 Review

This Policy shall be reviewed every 3 years by the policy owner, and may be amended, subject to approval, if deemed necessary at any point within the period of review.

2.23 Acknowledgement of Acceptable Usage Policy, Internet, and Email Usage

Each employee assigned a desktop, laptop, work, or mobile phone shall provide consent for the acknowledgement of the policy.

2.24 Acceptance of the Acceptable Usage Policy

This form is used to acknowledge receipt of, and confirm agreement with, United Capital PLC ("the Company") Acceptable Usage Policy.

2.24.1 Procedure:

1. Read the "Acceptable Usage Policy". If there are any aspects regarding this policy that are unclear, please consult the IT Manager.
2. Provide the consent that you have read and understand the policy by clicking **I Agree** menu in the consent form provided.
3. The consent list will be collated and forwarded to HR Department for record keeping purposes.

2.24.2 Consent/Signature

By signing below, I agree to the following terms: I have received and read a copy of the "Acceptable Usage Policy" and:

1. I understand and agree that any computer, software, and storage media provided to me by the Company contains proprietary and confidential information about the Company and its business and always remains the property of the Company.

2. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at the Company), or otherwise disclose, or allow any third- party copy or duplicate any of the information or software on any computer, software or storage media provided to me.

I agreed that, if I leave the Company for any reason, I shall immediately return to the Company the original and copies of all software, computer materials, storage media or computer equipment that I may have
received from the Company that is either in my possession or otherwise directly or indirectly under my control.
4. I agree to abide by the terms set out in the "Acceptable Usage Policy" and to be bound thereby. I understand and accept that in appropriate circumstances the Company may monitor and access the information, data, and e-mail on my computer.
5. I understand and agree that failure on my part to comply with the terms as set out in the "Acceptable Usage Policy" and this acknowledgement form may result in disciplinary action being taken against me.

THIRD PARTY INFORMATION SECURITY POLICY

1.0 Introduction

The Third-party Information Security Risk Management Policy is designed to assess and manage risks associated with engaging external parties that have access to UCAP's sensitive information or systems. This framework outlines standardized practices to ensure the confidentiality, integrity, and availability of data shared with or accessed by third parties.

1.1 Scope

This framework applies to all external entities, including vendors, suppliers, contractors, service providers, and any other third parties where sensitive information is shared, processed, or stored.

1.2 Objectives

- Identify potential security risks arising from third-party engagements.
- Assess and prioritize risks based on their potential impact on information security.
- Implement controls and mitigation strategies to manage identified risks effectively.
- Establish monitoring mechanisms to track and review third-party compliance with security standards.
- Ensure continual Improvement of security measures and risk management strategies.

1.3 Governance Structure

- Third-Party Information Security Officer: Appoint a designated TPISO responsible

for overseeing the Third-Party Information Security Risk Management Framework.

- Cross-Functional Team: Form a team comprising representatives from IT, legal,
procurement, compliance, and relevant business units to collaborate on thirdparty risk assessments.

1.4 Policy

- Cloud service providers must undergo a thorough evaluation process before selection for use within the Corporation. Evaluation criteria should include security controls, data protection measures, compliance certifications, vendor reputation, contractual commitments, and alignment with industry best practices.

• Conduct a proof of concept to assess the provider's capabilities, performance,
and compatibility with the Corporation's requirements. Test key functionalities, security controls, and integration capabilities during the PoC phase.
• Classify data stored and processed in the cloud based on its sensitivity level and impact on the Corporation. Apply appropriate security controls and encryption
mechanisms according to the data classification. Implement access controls to ensure that only authorized individuals can access and handle sensitive data.

• Conduct regular risk assessments to identify and mitigate potential security risks
and vulnerabilities associated with cloud services. Develop and implement risk treatment plans to address identified risks and ensure the security of cloud environments.
• Ensure that cloud services comply with applicable data protection laws and regulations, such as NDPR, GDPR, HIPAA, or industry-specific requirements.
• Provide employees with training on the secure use of cloud services, including
data handling, account security, and recognizing and reporting potential security incidents.
• Include provisions for data protection, confidentiality, service availability, incident response, and compliance with regulatory requirements in SLAs with cloud service providers.
• Communicate infrastructure amendments, changes to data storage procedures involving data migration to a different jurisdiction or global region, and the use of "peer cloud" providers or subcontractors with potential information security implications for the Corporation in advance.
• Periodically review this policy or as needed to reflect changes in technology, regulations, or business requirements.

1.5 Cloud Service Provider Selection Criteria

When selecting cloud service provider, it is important to conduct thorough due diligence and evaluate the potential provider against these criteria to ensure the selection of a reliable and secure partner for the Corporation:

1. Security Capabilities: Assess the cloud service provider's security measures, including data encryption, access controls, network security, intrusion detection and prevention systems, vulnerability management, and incident response capabilities.
2. Compliance and Certifications: Ensure that the cloud service provider complies with relevant regulations and industry standards, such as ISO 27001 for information security management or industry-specific compliance requirements (e.g., HIPAA for healthcare, PCI DSS for payment card data).
3. Data Protection and Privacy: Evaluate the provider's data protection practices, data residency options, data backup and recovery processes, and

their commitment to data privacy and confidentiality.
4. Service Reliability and Availability: Consider the provider's service-level agreements (SLAs) and track record for uptime, availability, and performance. Evaluate their disaster recovery and business continuity capabilities to ensure continuity of operations in case of disruptions.
5. Vendor's Reputation: Assess the provider's industry reputation, track record, and customer references. Consider factors such as the number of years in operation, customer satisfaction ratings, and any significant security incidents or breaches in the past.
6. Contractual Terms and Exit Strategy: Carefully review the contractual terms, including data ownership, data portability, termination clauses, and any limitations of liability. Ensure that there are provisions for data extraction, United Capital Plc- Information Security Policy Handbook Page 127 of 132 migration, and transition in case of changing providers or terminating the cloud services.
7. Vendor Support and Customer Service: Evaluate the provider's customer support services, including responsiveness, technical expertise, and availability for assistance during incidents or emergencies.
8. Scalability and Flexibility: Consider the scalability and flexibility of the cloud services offered, including the ability to adapt to changing business needs, accommodate growth and integrate with existing systems and applications.
9. Cost and Value: Evaluate the cost-effectiveness of the cloud services, considering not only the upfront costs but also any additional charges for data storage, bandwidth, support, or future expansions. Assess the overall value proposition, weighing the security features, performance, and benefits offered against the cost

Information Security for Supplier Management

1 INTRODUCTION

UCAP treats its information as a valuable asset and considers that it is essential that such must be protected, together with the systems, equipment and processes which support its use. These information assets may include data in electronic or physical form. In order to protect UCAP information appropriately, our contractors and third parties acting as suppliers must provide security measures and safeguards appropriate to the nature and use of the

information. All suppliers of UCAP must comply and be able to demonstrate compliance with relevant policies and standards.

2 OBJECTIVE

The management of UCAP is committed to the protection of the organization's assets and the provision of guidelines that suppliers must follow in accessing the organization's assets.

3 PURPOSE

This document sets forth information security policy that must be established in the handling, management, storage and processing of information assets belonging to UCAP by all UCAP suppliers to be maintained throughout the term of any arrangement between the parties. UCAP requires the security of its information to be maintained in order to ensure that UCAP is able to rely on its information for its business needs.

4 SCOPE This policy applies to all UCAP contractors, third parties, persons or organizations acting as suppliers.

5 POLICY

UCAP will assess the risk to its information assets and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the organization will require suppliers of services to sign a non-disclosure agreement to protect its information assets. A copy of the information security policies in ensuring compliance will be provided to suppliers prior to their being granted access.

Each supplier stated is categorized based on the information granted.

S/N	**CATEGORIES**	**TYPES OF ACCESS GRANTED**
1	Level 1	Servers, Server room, systems, and all critical information.
2	Level 2	Policy document, Active directory, and Remote Access
3	Level 3	General supply of information except critical information. e.g., Electronic Suppliers and other suppliers that are not critical

Before giving access to Level 1& Level 2 suppliers, suppliers MUST have an NDA signed, go through the third-party risk assessment framework, and provide necessary response before information disclosure. Level 3 suppliers do not need a signed NDA.

The criticality of Information security requirements for ICT products and services between a supplier and UCAP should have a Service Level Agreement (SLA) and NDA signed to prevent information leakage. Contact managers should meet with suppliers on a quarterly basis but if an urgent need arises, they can meet before the stipulated period.

Third-party risk assessment on relevant suppliers should be carried out on suppliers on a quarterly basis or when a service is needed. Information Security Department (IS)/Co-operate Services Department should carry out the assessment of relevant suppliers.

Suppliers should be contacted via email or contact numbers to verify if details given are still in existence.

For a supplier to be contacted for a particular service the supplier should have met he security requirements based on the nature and criticality of the product or service, should have carried out that particular service before, should have experience and must be competent.

UCAP Information assets include the following, regardless of the media in which it is contained:
• Any information relating to an identified or identifiable individual irrespective of
whether such individual is a UCAP. client, employee, or other status (such as name, address, email address, telephone number, date of birth, health or medical information, or any other unique identifier).
• Confidential non-public business information including any UCAP Confidential
Information as such term is defined in the non-disclosure agreement.
• Supplier's Security Program will include at minimum.

➢ Appropriate and applicable administrative and physical safeguards and other security measures designed to ensure the security and confidentiality of UCAP Information.
➢ Security design where applicable intended to prevent any compromise of its own information systems, computer networks or data files by unauthorized users, viruses or malicious computer programs which could in turn be propagated to UCAP.
➢ All persons with authorized access to UCAP Information must have a genuine business need-to-know prior to access.

5.1 Incident Notification Supplier will promptly notify (but in no event more than 48 hours after the occurrence) UCAP by telephone and subsequently via email of any potential or actual security attacks or incidents. The notice will include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being

taken to address the occurrence. A security incident includes instances in which internal personnel access systems above their user rights or use the systems inappropriately. Supplier acknowledges that it is solely responsible for the confidentiality and security of UCAP Information in its possession, custody or control.

i. End of Service The following process will be followed for end of service, early end of service or transfer of service to another party:

- The end of service will be requested in writing within the terms of the contract if one exists
- Transfer to another party (including in-house support) shall be planned via the Design and transition of a New or Changed Service process and change control procedures followed
- An assessment of the risk to IT service should be carried out prior to ending or transferring the service, and contingency plans put in place
- Any budgetary implications shall be incorporated into the financial model.

The various aspects of ending a service should be carefully considered at initial contract negotiation time in line with Section 2 of this policy document.

ii. Procedure for maintaining accuracy and completeness

1. Where possible, a written contract shall exist between all parties involved and UCAP L e g a l / Cooperate Services Department will hold a soft /hardcopy original signed by all parties which will also be scanned and held electronically

2. The contract shall include or contain reference to:
   a. The scope of the services to be delivered
   b. Requirements to be met by the external supplier
   c. Service level targets or other contractual obligation.
   d. Authorities and responsibilities of the Organization and the external supplier.

3. Regular formal communication is made with suppliers on a frequency dependent upon the amount of business conducted with the supplier and the importance of the goods or services to UCAP.

4. Any changes to the scope or terms of existing contracts are managed and documented fully via the change management process Soft/Hardcopy contracts will be stored within UCAP Legal/Cooperate Services Department.

5.2 Disclosure

Unless otherwise agreed by the parties in writing, Supplier shall not share, transfer, disclose or otherwise provide access to any UCAP Information to any other third party. Supplier will ensure that any approved third-party 11supplier

has information Security Program reasonably equivalent to that required of the Supplier as applicable for the services such third party provides.

5.3 **Ownership & Usage**

Any UCAP Information, including in any reconfigured format, will at all times be and remain the sole property of UCAP, unless agreed otherwise in writing by UCAP and supplier. Any usage of UCAP Information is limited to the sole purpose expressly authorized by the agreement.

5.4 Compliance

Supplier will comply with all applicable legal requirements (federal, state, local and international laws), rules and regulations and governmental requirements currently in effect and as they become effective, relating in any way to the privacy, confidentiality or security of UCAP Information.

5.5 **Secure Disposal**

Supplier will either return or dispose of UCAP Information upon contract termination or upon UCAP's direction which may be given at any time. Any disposal must ensure that UCAP information is rendered permanently unreadable and unrecoverable.

6 DISCIPLINARY ACTIONS

Violation of this guideline may result in disciplinary action, which is subject to management review and action in conformance with UCAP's disciplinary measures on breach of policy, guideline, standard, practice, and framework.

7 SUPPORTING DOCUMENTS

Reference #	Document's Name/ Detail
	Third-party Risk Information Security Risk Framework