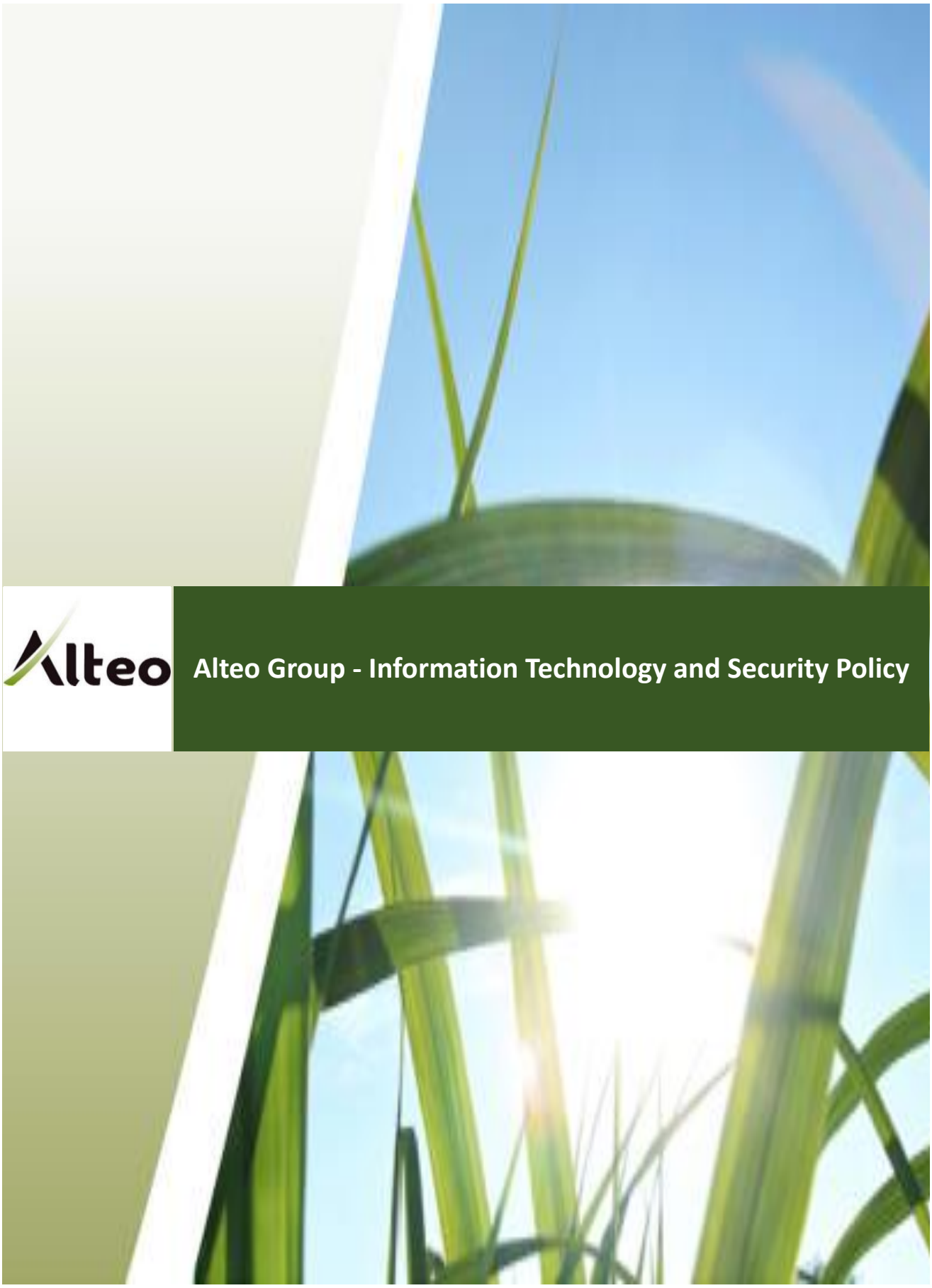

Alteo Group - Information Technology and Security Policy

TABLE OF CONTENTS

1 Information Technology and Security Policy

1.1 Introduction

Information security management is a key Information and technology (IT) governance responsibility, which is in turn a subset discipline of corporate governance. In line with the corporate governance strategy Alteo Limited, the Holding Company of Alteo Group, this document sets out the policies and controls related to information and technology usage and management of the company. The subsidiary, sister and venture companies of Alteo Limited, (hereinafter referred to collectively as "**Sector Companies**"), to which this policy applies to are herein listed in **Annex I**, hereto. Alteo Limited and the Sector Companies shall hereinafter collectively be referred to as "**Alteo**", the "**Group**" or the "**organisation**"),

1.2 Objectives

A vital business requirement of Alteo is the protection of its information assets with the following concepts:

Confidentiality
: Information is not provided or disclosed without authorisation

Integrity
: Accuracy and completeness of the information is maintained

Availability
: Information is made available to an authorised party upon request

The objectives of this information technology and security policy document are to:

Ensure that Alteo information systems safeguard and protect information assets

Provide a secure and structured information management framework to employees for the usage and protection of information systems and information assets

Ensure compliance with information security laws and regulations

Build an information security culture within the organisation

1.3 Non-compliance, Breach and Derogation

All Sector Companies and employees of the Group must comply with this policy and its guidelines.

Any breach of policy will be subject to investigation and a disciplinary process will follow depending on the type of the violation.

Derogation to the policy must be communicated by formal request to the Head of IT and Innovation with supporting arguments including but not limited to technical or procedural limitations or justifications. The derogation request will be reviewed, and decision communicated and documented.

1.4 Policy review

The policies shall be reviewed on yearly basis and changes subsequently communicated a finalised policy document, to ensure their continuing suitability, adequacy and effectiveness.

Each cluster IT manager shall submit their yearly reviews when applicable by the end of every third quarter of the Financial Year to the Head of IT and Telecoms.

Reviews shall be completed and changes approved by the board to be circulated by the end of every fourth quarter of the Financial Year every year.

2 Strategic Risk Management and IT Governance

2.1 Roles and areas of responsibilities

This section defines and allocates the information security responsibilities:

ITS Policy Guardian- The Head of IT and Innovation is the ITS Policy guardian and is responsible for the review, update and overseeing the compliance and implementation of the policy within the Group.

The Audit and Risk Committee- The ultimate responsibility for approval and effective implementation of the ITS Policy lies with the Audit and Risk Committee of Alteo Limited, which has been delegated by the Board of Alteo Limited to oversee the Group's risk management and internal control systems.

Cluster IT Manager - Each cluster IT manager in consultation with the ITS Policy Guardian commits for the effective implementation of the ITS Policy and adherence to the rules and guidelines through their respective IT Staffs.

Users and Third-party providers – Employees of the organisation and third-party providers who process information within or for the Group and interact with information systems must comply to this ITS Policy.

2.2 Segregation of Duties

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

In order to ensure separation of different functions, the authority and permissions of users and their respective access must be defined, approved and provided on the least privilege principle.

2.3 Security by design

The Group commits to the adoption of security by design principle for the implementation of information systems and technology infrastructure. The following guidelines must be adopted by all cluster IT managers:

Design

Security requirements must be formulated at the design phase of information systems and infrastructure solutions design.

Security testing

Information Systems and technology infrastructure components must be tested for security vulnerabilities before being put in production. Configurations must be audited and benchmarked against best practices.

Internet facing systems

Information systems and infrastructure components facing internet must be tested for penetration before being put in production.

2.4 Privacy and protection of personally identifiable information

The Group is committed to comply to The Data Protection Act 2017, which is itself aligned with the European General Data Protection Regulation (GDPR), and any other prescribes regulations, (hereinafter referred to as the "**Data Protection Laws**"). In this regard, the Group has adopted the required measures to comply with the Data Protection Laws.

3 Asset Management

3.1 Information Security Policy

Data must be protected at every level of the organisation within and outside the Group. The Group is therefore committed to the implementation of an effective information security policy to mitigate risks of data leaks and data breaches.

3.1.1 Classification of information

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

Classification	Description	Examples include but not limited to
Sensitive	Information that is of the highest level of importance for the Group. Such information if disclosed can adversely impact the Group's reputation and/or cause prejudice to the business	Strategic business agreements, minutes of board meetings, business plans
Confidential	Information that is disclosed on a need to know basis and through authorisation internally. Such information can cause prejudice to the Group in case of unauthorised disclosure to third parties	Client payment records, company developed software code, IT systems documentation
Internal	Information is restricted to within the company only and protected from unauthorised access to third-party	Company policies, standard operating procedures, client contact information
Personal Data	means any information relating to an identified or identifiable natural person, including special categories of data, who can be identified, directly or indirectly, in particular to an identifier.	Identity Data, Contact Data, Remuneration, Health Information, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
Open	Information is not confidential and can be made public without any implications for the Group	Marketing materials and/or product brochures, published financial reports, newsletters

3.1.2 Labelling of information

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the Group.

3.2 Tangible IT assets

The various types of IT Assets associated with information processing facilities within the Group shall be identified and an inventory of these assets should be drawn up and maintained. Such assets shall comprise of but not limited to hardware, software, licenses, and cloud services.

3.2.1 Inventory, ownership and renewal of assets

Each cluster IT manager must keep an inventory of critical infrastructure components in order to keep track of the quantities, locations, patching status, vulnerabilities, end of support, equipment retirement plans and replacement plans.

3.3 Removable Media Management

Removable media refers to any form of storage that is designed to be inserted or connected to a system and removed or disconnected with the aim of storing and transporting data. Examples of removable media include but are not limited to Universal Serial Bus (USB) drives, optical disks (CDs, DVDs, Blu-ray Discs), magnetic tapes, smart phones, music players and similarly equipped handheld devices.

While removable media and devices are extensively used for backup, storing and transporting data, some of the characteristics that make them convenient can also introduce security risks to the Group. Such risks include data security, malware infections, copyright infringement and hardware failures. The following guidelines must be adopted by all users as a proactive approach in risk reduction:

- Use only trusted and company approved external drives
- Ensure external drives are encrypted and password protected
- Report stolen or lost removable media the soonest possible through the appropriate channel

IT staff must ensure the following controls are in place:

- Anti-malware software is installed and updated for all user workstations with automatic scanning enabled.
- Autorun and Autoplay features for all removable media or devices are disabled
- Backup media are encrypted, and such media are stored in a physically secured offsite facility
- Removable media shall be disposed of securely when no longer required, using the formal procedures established within the Group

4 Access Control

4.1 Access control policy

The Group implements physical and logical access controls across its networks, IT systems and services in order to control the identification, authentication and authorisation of users.

Identification is the process through which a person is identified to the information environment and should be based on user access accounts which need to be unique and defined based on user's identity.

Authentication is the process of users identify verification. Authorisation is the process of granting access to services for which the users have been authorised to use.

4.2 Access to networks and services

The Group's users will be provided access based on the least privilege principle with access limited to only authorised rights and resources.

4.3 User access management

User accounts must follow the organisation's username convention as authorised for each Sector Company. The following conventions have been authorised for the Group:

Alteo Limited	Use the first letter of the user's first name and the last name of the user to create the username
Agri & Indus Cluster	
Anahita Estates Limited	
Anahita Golf Ltd	Use the first name and the last name separated by a "." to create the username
Anahita Residences & Villas Limited	

Assignment of access rights shall follow the Group's formal user registration and de-registration procedure.

Account lockout is a mechanism which keeps access accounts secure by preventing anyone or anything from guessing the username and password. When the account is locked, the user must wait for an amount of time before being able to log into your account again. Account lock must be implemented for a tolerable number of failed attempts.

Idle timeout is a mechanism that prevents a user's session from remaining active indefinitely by automatically signing out the user after a certain period of user inactivity. Idle timeout must be implemented for a defined period of inactivity.

Default access accounts should be removed or disabled as far as possible. For such systems which do not allow removal or disabling of default usernames, such accounts should be set with a highly complex password and reserved for emergency use only.

Access to the Group's information processing facilities accessible through the internet must be protected by a two factor authentication mechanism.

4.4 Privilege access rights management

Usernames with administrator rights and other privilege access rights must to be defined differently from standard user logins. The allocation and use of privileged rights shall be restricted and controlled.

4.5 Review of access rights

Each cluster IT manager has the responsibility of performing users' access rights review at regular intervals, with at least one review per year.

The access rights of all employees and third party users (if applicable) to the Group's information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon charge.

4.6 Password management policy

This policy provides guidelines for the consistent and secure management of passwords and is applicable but not limited to user-level access, system-level access and service accounts.

The following guidelines must be followed:

Blank or predictable passwords (such as "password", "12345", "qwerty" or "p@55w0rd") are not permitted for any account, no matter how trivial. Passwords should also not contain dictionary words.

Password must have a minimum level of complexity, containing at least eight alphanumeric characters and a mixture of lowercase, uppercase, numbers, and special characters (such as !@#$%^&*).

Different passwords should be used on different systems.

5 User Responsibilities

5.1 End user policy

Employees are expected to know, understand, and abide by the Group's policies in their daily use of technology and information processing facilities. Such facilities include but are not limited to:

- End user devices such as workstations, laptops, printers, fax machines etc.
- Email
- Cloud services or applications
- Corporate phone and video conferencing facilities
- Social media
- Instant Messaging

In line with the Group's guidelines, employees are expected to uphold the standards and principles of the Group by acting responsibility and respecting the rights of others at all times in the daily use of technology and information processing facilities.

5.2 Acceptable use policy

The acceptable use policy is an integral part of the ITS Policy of the Group aiming at protecting employees from inappropriate use of technology and information processing facilities that may expose the Group to risks including malware infection, compromise of network systems and services, data breach and legal issues.

General use and ownership:

Corporate data stored on electronic and corporate systems whether owned or leased by, the employee or a third party, remains the sole property of the Group. Users must ensure through legal or technical means that such data or information is protected in accordance with this policy. Users have the responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

Users may access, use or share confidential or sensitive information only to the extent it is authorized and necessary to fulfil their assigned job duties.

Unacceptable use:

- Sharing of usernames and password.
- Users must not write passwords down or send passwords through email and/or instant messaging services.
- Upload, post, transmit or otherwise make available any material that may harm the Group's reputation.
- Send, transmit, or otherwise distribute sensitive and/or confidential information, data, trade secrets or other proprietary information belonging to the Group without the proper authorisation.
- Send unsolicited emails including junk mails or spam mails related to advertising.
- Indulge in any form of harassment via email, messaging services, video, and telephone or through the use of any other information and communication technology equipment.
- Indulge in online defamation where false and/or damaging statements are made about another person or organisation through email, message boards, blogs, chatrooms, or any other Internet based communication medium.
- Use, or forge, unauthorised email identity or header information.
- Initiate and/or circulate non-business-related messages to large number of users through newsgroups without authorisation
- Tailgating, bypassing security controls or obtaining administrative privileges on systems without authorisation
- Use or install unauthorised, cracked or pirated software on company systems
- Excessive download of unauthorised including but not limited to as music, video, software, and other copyrighted files from the internet.
- Accessing web sites that are not business related and subsequently consume internet bandwidth negatively impact other legitimate business related activities.
- Accessing web sites with inappropriate content including but not limited to malware, adult content, hacking, extremist groups, proxy avoidance, gambling
- Sharing of potentially harmful digital content within the Group or to Group employees through any channel. Examples include are not limited to Universal Serial Bus (USB) drives, optical disks (CDs, DVDs, Blu-ray Discs), magnetic tapes, smart phones, music players and similarly equipped handheld devices.

5.3 Internet usage policy

The Group provides internet access to users to support the business functions and only as needed for employees to fulfil their duties. All users have a responsibility towards fair usage of company resources and should therefore exercise good judgment in using the Internet.

Users must therefore refrain from activities falling under the "unacceptable use" category during the usage of internet facilities.

The Group reserves the right to monitor or block any internet access deem to potentially represent a risk to the security of the organisation's information processing facilities and information assets.

5.4 Clear desk and clear screen policy

The Group's clear desk and clear screen policy is in line with its objective to comply to Data Protection Laws and reduce the risk of information theft, fraud, or a security breach that may be caused by sensitive information being left unattended and visible in plain view.

- Users must ensure that confidential or sensitive information in their possession remain safely kept and locked when not in use.
- Documents containing confidential or sensitive information should be disposed properly using a paper shredder.
- Printers, photocopiers and/or fax machines are clear of papers as soon as they are printed.
- Whiteboards should be erased and flipchart sheets disposed after usage.
- Users should avoid keeping documents and files on computer desktops rather store files in folders located in authorised secured locations.

6 Physical and environmental security

Effective physical security measures help protect against unauthorized access, damage, or interference in areas where critical or sensitive information is prepared or located, or where information processing services supporting key business processes are carried out. Example of such areas are but not limited to user workspace, server rooms, data cabinets, and remote offices.

Adherence to this policy is required in ensuring the security of the Group's information assets, the protection of the interests of the Group, its personnel and customers.

6.1 Workspace security

It is the responsibility of the appropriate individuals to enforce appropriate procedures by ensuring only authorised persons are allowed into areas that house confidential or sensitive information or information processing resources.
Visitors must be screened based on their purpose to access the premises and accompanied within workspaces by Group personnel.

6.2 Server rooms security

Server rooms shall be equipped with the appropriate controls for protection against external and environmental threats. Such controls are but not limited to:

- raised flooring
- adequate ventilation and temperature control
- Automatic fire suppression
- Temperature, humidity and fire alarms CCTV monitoring

Data cabinets must be locked at all times when not in use.

Cables must be properly managed with appropriate accessories where required.

Cables and equipment must be labelled. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

6.3 Security of equipment on premise and off premise

Security shall be applied to both on premise and off premise assets such as workstations, laptops, external drives, memory cards, mobile phones, and tablets.

Workstations, laptops, and mobile devices shall be protected through:

- passwords or pin codes
- Automatic screen lock

Users shall ensure that unattended equipment are secured appropriately as external drives, memory cards and portal computers are often the target of thieves.

7 Operational Security

7.1 Change management policy

The purpose of this policy is to manage changes that occur to information processing facilities in a way that minimises risk and impact to the confidentiality, integrity and availability of information.

Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled. Changes shall follow a process of planning, evaluation, review and approval.

7.2 Capacity management policy

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required performance of information processing facilities.

7.3 Logging and Monitoring

Event logs recording exceptions, faults and information security events shall be regularly reviewed.

Logging facilities and log information shall be protected against tampering and unauthorised access.

7.4 Restrictions on software installations

Installation of unauthorized computer programs and software, including files downloaded and accessed on the internet, can easily and quickly introduce serious, fast-spreading security vulnerabilities. Unauthorized software program from untrusted sources can introduce malware to the Group's information processing facilities. As such adherence to the software installation policy of the Group serves a critical role in the process of security the Group's information ecosystem. All users must therefore abide by the Group's guidelines for software, program, and application installation.

7.5 Malware protection

All information systems including but not limited to workstations and servers, whether connected to the company network or as a standalone, must use an approved company protection software.

Endpoints must be equipped with the latest generation of anti-malware protection with advanced threat protection for the efficient detection and extraction of latest malware. Workstations and servers malware scanning must be configured with appropriate schedule for weekly scans.

Network devices such perimeter firewalls and core firewalls must be equipped with Advanced Threat Protection for the emulation and extraction of malware at network level.

The email system shall also be protected with Antispam for filtering of unwanted messages.

Advanced Threat Protection for the emulation and extraction of malware in email attachments, and inspection of web links for malicious content.

7.5 Technical Vulnerability management

Information systems must be scanned for vulnerabilities on regular basis. Any new system must be scanned for vulnerabilities and appropriate measures taken to address the associated risks before put into production.

7.6 Information Security and Human Resources

The contractual agreements with employees and contractors should state their responsibilities for information security.

Background verification checks on all candidates for employment must be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and perceived risks.

Each Sector Company shall ensure through appropriate procedures that employees return company assets upon termination of their employment, contract or agreement and access to the Group's information processing facilities and systems are duly terminated.

The Group shall conduct security awareness sessions regularly to educate and test employees to help protect the Group's business against cybercrimes, including phishing and other social engineering attacks.

8 Network and Information Transfer Security

The purpose of this policy is to establish the guidelines and controls necessary for a secure network infrastructure. Networks shall be managed and controlled to protect information held by the information processing facilities within the Group.

8.1 Network Security Management

The network must be designed in such as way that it provides segregated between users, servers, Demilitarised Zones (where applicable) to provide granular control traffic between different zones.

A firewall must be used to provide perimeter security between the internet and the internal networks. Firewalls must be configured with appropriate rules and the rules follow the least privilege principle.

Guest wireless networks and mobile devices networks shall be segregated from internal networks either physically or through the use of a firewall.

All Wi-Fi access points allowing connectivity to the Group's network should use the strongest available and feasible encryption mechanism to secure transmissions with wireless clients.

Authentication to internal Wi-Fi networks should be through strong passwords and changed on a periodic basis. The maximum lifetime of a Wi-Fi password must be ninety days and not more.

Alteo recommends that all Company Confidential Data which employees consider sensitive and/or vulnerable, be password protected or, where feasible, encrypted. In case of doubt as to the nature of the information, and the need for protection or encryption, the higher level of care should be preferred, and password protection or encryption should be set with respect to such information.

The use of unencrypted protocols is not authorised for the transmission of information within the Group.

Unauthorised devices including but not limited to port scanners and rogue access points are prohibited on the corporate network.

8.2 Email policy

Remote access to email or webmail shall be provided only to users strictly requiring remote access to their mailbox.

MFA (Multi-Factor Authentication) on webmail (for example Microsoft Office 365 OWA) shall be enabled for all users requiring access to their webmail.

Emails from server to server must be encrypted by default.

Password aging will be enforced particularly in cases where MFA is not enabled.

Password history must be enabled to prevent reuse of recently used passwords.

8.3 Portable computer devices and teleworking policy

The Group shall adopt security measures to manage the risks relating to the use portable computer devices. Such measures shall include but not limited to the following controls to ensure portable devices are compliant when they connect to the Group's information processing facilities:

- The Group's domain policies are applied to the devices
- Anti-malware software is installed and enabled on the devices
- The disks are encrypted
- The Group's web policies are applied and enabled on the devices to protect them from web sites with inappropriate or harmful content

8.4 Cloud usage policy

Cloud services are services identified as resources made available through the internet for storing and/or processing of data.

Cloud services can be available:

Free of charge.

Example of such services are Gmail, Dropbox, iCloud, OneDrive and so on.

Billable services

Such services come in multiple flavours. For example IaaS, SaaS, and PaaS.

Only the Group's authorised cloud services shall be used by users for storing and processing of corporate data.

Cloud services shall also be subject of security audits to ensure they comply to the Group's security requirements.

8.5 Remote access policy

This policy defines the acceptable methods of remotely connecting to the Group's internal network from untrusted external location such as internet, free Wi-Fi networks, other offices or abroad.

Any remote access to the Group's internal network shall be provided through an encrypted connection (Virtual Private Network) and access managed through firewall policies.

Portable computers connecting to the internet network through remote access must comply to the portable computer devices and teleworking policy.

Access to the Group's internal networks should be authorised for approved users and such access reviewed on regular basis.

Providing remote access to the internal network through freeware such as TeamViewer and GoToMeeting shall be temporary, on requirement basis, following an approval and strictly under supervision of appropriate Group's staff.

8.6 Bring Your Own Device Policy

"Bring Your Own Device" commonly known as BYOD refers to the concept of employees using their personal devices to connect to corporate network to access digital services such as email and internet for web browsing.

The Group has adopted a BYOD policy by providing its employees the privilege of purchasing and using smartphones and tablets of their choice at work for their convenience. The Group however reserves the right to revoke this privilege if users do not abide by the Group's policies and procedures.

Employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network. Users must therefore:

- Use their devices in an ethical manner at all times
- Adhere to the Group's acceptable use policy and
- Refrain from activities falling under the "unacceptable use" category during the usage of their personal devices.

8.6.1 Supported devices and enrolment

Smartphones, tablets, iPads are allowed.

Users must request for access and present their personal devices to their respective IT departments for enrolment.

Employees may use their mobile device to access the publicly available company-owned resources such as email, calendars and contacts. Connection for BYOD devices shall be provided through a segregated network and access to internal network strictly prohibited.

8.6.2 Risks and liabilities

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.

The Group reserves the right to install its own antivirus on the employee's mobile device or request the employee to install a specific antivirus under the IT department's supervision. Regular checks will be done by the IT department to ensure that security is maintained concerning those devices.

The Group reserves the right to disconnect devices, disable services without notification or wipe any corporate data stored or found on the BYOD devices if there is threat to the safeguard and protection of its information assets.

9 Backup Policy

The purpose of this policy is to provide the guidelines for the continuity, restoration and recovery of critical data and systems in the event of a system failure, accidental or intentional deletion or corruption of data, or disaster.

9.1 Categories of business critical data

The following categories of business data have been identified as critical which need to be saved to a secure media for preventing any loss in the eventuality of unavailability:

- Corporate Files

  Corporate files are documents in digital format, which contain information necessary for pursuing the Group's business functions and activities. Example of such files include but are not limited to financial records, customer records, email records, address books, business agreements, and intellectual property documents.

- System Resources and Images

  System resources and images are critical components of or complete information systems deemed as critical for business operations. Such system resources or images which include but are not limited to virtual machines, servers, system files, software applications, device drivers, firmware, patches and hotfixes.

- Configuration Files

  Configuration files are files containing system instructions or parameters commonly referred to as settings that are used by computer programs and devices to function. Configuration files are critical components as they provide the ability to restore information systems rapidly without the need for undergoing complete system rebuild which is a time consuming process.

- Databases

  Databases are electronic systems that provide digital software structures for storing, managing and retrieving information.

9.2 Backup Process

Recovery Point Objective (RPO) is a measurement of time usually in minutes or hours that determine the maximum acceptable amount of data loss. RPOs are determined and based on the frequency of backup. In other words, higher backup frequencies provide most up to date version of data.

Each cluster IT manager is responsible for:

- The identification of business critical data and respective data locations that must be secured through a backup process.
- Aligning respective backup schedules with the Group's RPOs.
- Ensuring backup procedures are executed in a timely manner to achieve the Group's RPOs.

9.2.1 Backup schedule

The following guidelines are applicable for backup schedules:

- Backups must be executed after regular business hours.
- Full backups shall be scheduled during weekend hours
- Incremental or differential backups shall be scheduled on daily basis
- Simultaneous backup schedules shall be avoided as much as possible.

9.2.2 Backup retention

Backups shall be retained as per procedures.

9.2.3 Offsite backup

Weekly full backups shall be secured to an offsite location on regular basis.

9.2.4 Integrity testing and monitoring

Each cluster IT manager must ensure:

- Random backup restore tests are conducted on regular basis
- Full backup restore tests are conducted as per procedure
- Backup is monitored through logs and details of restore tests documented

10 Incident Management Policy

The incident management policy provides the framework for the reporting of and effective response to information security incidents within the Group.

This policy applies to all the Group's users, sub-contractors and business partners who have access to the Group's information processing facilities and/or confidential or sensitive data.

The Group defines a security incident as an event which violates it's ITS Policy and/or indicates that the Group's information systems or data have been compromised and/or that security controls put in place to protect the Group's information have failed.

Examples of security incidents include but are not limited to the following:

Loss or theft of any equipment storing confidential or sensitive corporate data
Malware infection on laptops or any other systems
Compromised user accounts
Suspicion or signs of third party being able to log in user's account
Unauthorised access to offices, server rooms, data cabinets or information systems

10.1 Incident discovery and containment

Information security events shall be reported through appropriate management channels as quickly as possible and the Group's Head of IT and Innovation promptly notified.

Incidents shall be examined based on their origin and causes, time of occurrence, extent of damage, and impact.

Containment measures shall be subsequently taken to mitigate the impact of the incidents on the confidentiality, integrity and available of data.

10.2 Incident eradication, recovery and communication

The Group shall implement a procedure for effective security incident eradication, recovery and communication.

11 Business Continuity Management

11.1 Business Continuity management policy

The Group shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

11.2 Critical Business Functions

Each Sector Company shall determine its requirements for information security and the continuity of information security management in adverse situations such as but not limited to technological issues, natural disasters or infrastructural problems impacting business operations.

11.3 BCP Review

Each Sector Company shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

12 Supplier Relationship Management

Information security requirements for mitigating the risks associated with supplier's access to the Group's information assets shall be agreed with suppliers and documented.

Agreements with suppliers shall include requirements to comply to the Group's ITS Policy and Data Protection Policy.

13 Induction and Training to IT Policy

The IT department shall assist new employees as part as their induction to the Company IT Policy. The new employees shall have a brief explanation concerning the different security measures and practices to be adopted while using the Company IT assets and software. Where applicable, training will be offered to facilitate the proper use of software and applications the employees are expected to work with.

Training and refresher courses are part of the program instituted by the Company to ensure that the development of the employees. The IT department shall ensure that any all computer programs installed are complemented with an appropriate training, either supplied by the IT Department itself or a Service Provider/Consultant.

The IT Department shall ensure that employees are regularly reminded of the proper practice of the IT Policy using different methods such as eLearning trainings, informational emails, or focus group meetings.

14 Glossary of Terms

Keyword	Description
ITS	Information Technology and Security
Policy guardian	Refers to the role and responsibility of updating and maintaining the policy document accurate and aligned with the group's corporate governance strategy.
Cluster IT Manager	Position held by appropriate persons with responsibility of managing IT and security risks within each company or entities within the Group.
Users	Employees, trainees, permanent or temporary staff, business partners, subcontractors or any authorised person by the group to interact with the group's information processing facilities or process information for the group through its information systems.
USB drive	A USB (Universal Serial Bus) drive is usually a data storage devices users can connect to their computers to transfer data.
Magnetic tapes	Tape used in tape drives for storing of digital data, usually used for backup purposes
Malware	Refers to any malicious software that is harmful to a computer systems and users. Example of malware are computer viruses, Trojan horses, spyware, ransomware, computer worms.
Anti-malware	Software intentionally designed to detect and remove malware from computer systems
Autorun	Feature in Microsoft windows systems that cause common media types such as CDs, DVDs, USB drives and so on to be triggered automatically
Endpoint	Computing devices that connect to the network and interact with users. Example workstations, laptops, printers and so on.
Tailgating	Entering into a secure area by closely walking behind another user hence bypassing the security control while the door is open
Cracked	Refers to software which have been subject to particular manipulations for truncating their licenses
Proxy avoidance	Refers to websites or software that allow users to browse websites without being detected by network security controls.
Emulation	Refers to the function of reproducing the action related to a particular suspected content in view of determining its impact
Advanced Threat Protection	Refers to state of the art capability of information systems to combat malware through advanced techniques
Perimeter firewall	Security control point installed between the internal network and internet
Core firewall	Security control point installed within the internal network for control of traffic between different network segments
Phishing	Refers to the fraudulent attempt of obtaining confidential information from users through tricks over phone calls, emails or even text messages
Antispam	Refers to mechanism used to filter unwanted emails based on their content, sender's reputation and other criteria
Social-engineering	Refers to psychological manipulation of people into performing actions or divulging confidential information

Demilitarised Zone	Refers to network security concept of segregating network resources to which external access is provided
Port scanners	Refers to computer programs designed to inspect computer systems for available services called “ports”.
Rogue access points	Refers to a wireless access point that has been installed on a secure network without explicit authorization from a local network administrator
MFA	Refers to Multi-Factor Authentication which is a security mechanism designed to authenticate users after they have provide two or more evidences of their identity.

End of Policy Document