Process Information Technology

Procedure IT Policy

Rev	Written by	Reviewed by	Approved by	Effective Date
A	Nguyen Truong Son	Herve Boone	Herve Boone	Dec 2007
B	Nguyen Truong Son	Herve Boone	Herve Boone	Dec 2009
C	Nguyen Thien Loc	Herve Boone	Herve Boone	August 2013
D	Nguyen Thien Loc	Herve Boone	Herve Boone	1st April 2014
E	Nguyen Thien Loc	Herve Boone	Herve Boone	1st Nov 2015
F	Damien Couribu	Jean-Pierre Mazzone	Cyrille Dreuillet	1st Jan 2019

Revision tracking:

Rev	Change Date	Content of change
F	1st Dec 2018	Creation of IT Regulation Committee and various updates

Transmitted for application to:

- Information Technology Managers
- Human Resources Managers

Transmitted for information to:

- All employees

1. Introduction

1.1 Purpose

The purpose of this policy is to outline the acceptable use of IT equipment and services provided by Archetype such as computers, servers, network, hardware, software, email, internet, etc. It gathers IT rules in use at Archetype, applicable to all employees and collaborators regardless of their location, either in or outside Archetype premises. It also applies to non-Archetype IT equipment and software brought by employees and third party within Archetype premises.
These rules are in place to protect the employee and Archetype. Inappropriate use exposes Archetype to risks including virus attacks, compromise of network systems and services, and legal issues. Effective security is a team effort involving the participation and support of every Archetype employee and affiliate who deals with information and/or information systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

1.2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Archetype business or interact with internal networks and business systems, whether owned, leased by or loaned to Archetype, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Archetype and its subsidiaries are responsible for exercising good judgement regarding appropriate use of information, electronic devices, and network resources in accordance with Archetype policies and standards, and local laws and regulation.
This policy applied to employees, contractors, consultants, temporaries, outsourced and other workers at Archetype, including all personnel affiliated with third parties and visitors. This policy applies to all equipment that is owned, leased by or loaned to Archetype.

1.3 General policy statements

All employees have no expectation/rights of privacy in anything they create, store, send or receive on Archetype systems. For example, their emails can be monitored without prior notification if deems necessary. If there is any evidence that an employee is not adhering to the guidelines set out in this policy, the company reserves the right to take disciplinary action, including termination and/or legal action.

1.4 IT Regulation Committee

As mentioned in this policy, there are a few cases where Archetype could decide to access employee mailboxes, files or any log of activities. Since employee privacy is Archetype utmost concern, any such investigation should be discussed and agreed by an internal committee composed at least of:

- Direct manager of the employee
- Department director
- Country HR manager
- Country managing director
- Group HR director

In case the employee is a director, all this committee is formed by all the ComEx members.
IT employees are not allowed to consult any private communication without prior approval of the committee.

2. Hardware

2.1 Definition and responsibilities

All hardware devices acquired by through purchasing shall remain Archetype property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts and agreements.
Any employee or collaborator who is entrusted with hardware is responsible for taking good care and protecting it from any damage, loss, theft or improper use and for returning it in good condition at the end of its use. It is strictly forbidden to anyone to proceed with the opening, modification, upgrade or downgrade of any hardware belonging to Archetype.
Any defect or breakdown shall be promptly notified to the IT Manager. Users of handheld devices and laptop computers must take active precautions to minimize the risks of theft or data tampering of malicious attacks.
Storage of business data on local hard drives is discouraged except if properly synchronised with OneDrive to ensure proper backup. The user must be aware that data security is one of their prime responsibilities.
Copying files on USB keys, CDs, etc., is strictly forbidden unless authorized by a Manager. In case of loss, damage or theft of a company's equipment due to the fault or negligence of its user, the user will be responsible to replace it at his/her expense.

2.2 Purchasing

All purchasing of company computer hardware devices shall be centralized within IT department to ensure that all equipment conforms to Archetype hardware standards and is purchased or leased at the best possible price.
All requests for hardware devices must fit within IT budget and be approved by the Managing Director. The request must then be sent to IT Manager, who will then review the need for such hardware and then determines that such hardware is needed.

2.3 Standards

The hardware standard list is the typical hardware configuration for new computers. It is available at this address: Computer Specifications.docx
Employees will be given access to appropriate network printers. In some limited cases, employees may be given local printers if deemed necessary by the Manager/Director in consultation with IT department.
Employees needing computer hardware other than what is stated above must request such hardware from IT department. Each request will be considered on a case-by-case basis in conjunction with the hardware purchasing section of this policy.

2.4 External equipment

No outside equipment may be plugged into the company's network without IT department written permission.

3. Software

3.1 Definition

All software acquired for or on behalf of the company or developed by company employees or contract personnel on behalf of the company, is and, at all time, shall remain as company property. All such software must be used in compliance with applicable licenses, notices, contract, and agreement.

3.2 Purchasing

All purchasing of company software shall be centralized within the IT department to ensure that all application conform to corporate software standards and are purchased at the best possible price.
All requests for corporate software must be submitted to IT department and sent to Finance and Managing Director. The IT Manager will then review the need for such software, and then determine the standard software that best accommodates the desired request.

3.3 Installation

IT employees are the only persons authorized to install and remove any software (either free or not) on any Archetype computer. Anyone offending this basic principle will be subject to the most severe sanctions, including immediate termination. For security reason, the Administrator profile of all Archetype computer belongs and is managed only by the IT department.
Shall the installation of new software be necessary, its installation must be requested in writing by the employee's manager and validated by the Managing Director. Upon approval, the IT Manager will organize the purchase of the license and the installation of the software upon its reception. If the software is free, it must be verified and tested by IT department before getting approved by Managing Director.
Usage of portable software (which doesn't require installation) **is forbidden** in all case. It is also strictly forbidden to install or play any offline or online games, or to download any music or movie.
Personal software or applications developed and used for performing calculations to be used in the design process, such as spread sheets, must be first checked for compliance with this IT policy regarding software/hardware compatibility and then quality assurance checked by the divisional or senior manager for technical correctness prior to approval of its use on Archetype projects.

3.4 Licensing

Each employee is individually responsible for reading, understanding, and following all applicable license, notices, contracts, and agreements for software that he or she uses or seeks to use on company computers. If an employee needs help in interpreting the meaning/application of any such licenses, notices, contracts and agreements, he should contact IT department for assistance.
Unless otherwise provided in the applicable license, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of copyright law. Therefore, it is strictly prohibited to use Archetype license on personal computers.

3.5 Standards

The list of standard suites of software that can be installed on company computers and fully supported by the IT department can be found at this address: Software Standard List.xlsx
Employees needing software other than those programs listed above must request such software from IT department. Each request will be considered on a case-by-case basis in conjunction with the software purchasing section of this policy.

4. Bring Your Own Device

At Archetype, we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to Archetype's network and equipment. We encourage you to read this paragraph in full and to act upon the recommendations. This policy should be read and carried out by all staff.

4.1 Definition

Bring Your Own Device refers to the use of personally owned notebooks, smartphones, tablets and any other types of mobile devices for business purposes.

4.2 Policy

It is strictly forbidden for anyone to bring and use any personal devices, except smartphones, in Archetype premises. It is therefore absolutely forbidden to connect to Archetype's network with a personal computer.
The use of smartphones and tablets is permitted to access business email or Intranet as well as making phone calls. Installation of needed applications (Microsoft Outlook) can be supported by IT.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device.
- Not to use the registered mobile device as the sole repository for Archetype's information. All business information stored on mobile devices should be backed up (using OneDrive).
- To make every reasonable effort to ensure that Archetype's information is not compromised using the mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.
- To maintain the device secured and up-to-date.
- Not to share the device with other individuals to protect the business data access through the device.
- To notify Archetype immediately in the event of loss or theft of the registered device.
- Not to connect USB memory sticks from an untrusted or unknown source to Archetype's equipment.

4.3 Teleworking

The use of mobile devices will be controlled by a strict authorisation and inventory process which will be subjected to regular audit. Staff who are required to work remotely or use portable devices will be issued with suitable equipment meeting Archetype security information requirements and local technical standards.
Only equipment meeting current Archetype security requirements will issued to staff. All security features will be fully activated before the devices are issued.
All portable devices will be uniquely identified and registered in Archetype and services provider asset register. Staffs are required to comply with security policy procedures when using or transporting the devices.
This policy will be subject to annual review or as required due to local incidents or changes in Archetype security standards.

5. Password

All passwords are initially set up by IT Manager and provided to the user. Upon first-time usage, a change will be requested to the user, who is then responsible to remember it.
For emergency action and upon request of the Management, IT Manager can reset employee password in order to be able to submit to a third party.

5.1 Password rules

- Minimum length: 8 characters
- Minimum complexity: must use three among four of the following types of characters:
  - Lowercase
  - Uppercase
  - Numbers
  - Special characters such as "!@#$%^&*(){}[]"
- Passwords are case sensitive
- Maximum password age: 90 days
- Account lockout threshold: 5 failed login attempts
- Reset account lockout after 30 minutes
- Account lockout duration: 30 minutes
- After a period of inactivity, each computer will automatically be locked-out and should be unlocked by entering user password. However, computers should not be unattended with the user logged on and employees are to not leave their computers unlocked. Quick lock can be performed by pressing Windows + L keys.

5.2 Password protection

- Never write passwords down on paper or on electronic document.
- Never send a password through email.
- Never tell anyone your password.
- Never reveal your password over the telephone.
- Never fill your password on a form on the internet if it is not 100% sure source.
- Never use the "Remember Password" feature of internet browsers or any other.
- Never use your Archetype password for another personal account.
- Report any suspicion of your password being stolen to the IT Manager.
- If anyone asks for your password, please contact with IT Manager first.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily distinguishable such as phone number, birthdate, etc.
- Be careful about letting someone see you type your password.

5.3 Phishing

Phishing is the fraudulent attempt to obtain confidential information such as password or user account by faking identity and disguising. This kind of attacks have increased dramatically in the past months and become more and more difficult to discern.
Extra precaution is therefore asked to all employee when entering their login and password on Internet. There is no chance that Microsoft will contact you directly about problems on your email account. Any suspicious request should be informed to IT Manager before taking any action.

6. Email

6.1 General

When using company resources to access and use the Internet, users must realize they represent the company. All emails sent and received are the property of Archetype. Users should not expect that emails are confidential or private even so it will usually be the case.
Users should exercise good judgment and common sense when creating and distributing email messages in order to limit email exchanges. In particular:

- Emails should not be sent for matters requiring a reply from the recipient within less than 24 hours. Phone or instant messenger should be used instead.
- When receiving an email, the use of "Reply all" should be limited to specific cases where all potential recipients are interested in the reply. Otherwise only specific users potentially interested should be selected.
- Project related emails should be sent through a dedicated document management system (eProject) when available. When such system is not used, a copy of the email should be sent to a dedicated email box, created at the beginning of each project (project.xxx@archetype-group.com where xxx is the project acronym).

Archetype retains the right to access or view employee's emails. This right will only be exercised when the company genuinely believes that the user has not complied with this policy. IT Regulation Committee is the only group of persons authorized to access another employee's emails. However, IT Director/Manager will browse logs (not email content) when alerted by abnormalities to mail traffic patterns and might disclose it to the Management.

6.2 Prohibited use

It is strictly forbidden to:

- Write, send or forward emails containing abusive, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.
- Forward a message or copy a message or attachment belonging to another user without acquiring permission from the originator first.
- Send unsolicited email messages, spams or chain mail.
- Forge email messages, disguise or attempt to disguise your identity when sending mail.
- Send emails of harassment, intimidation or unwanted invasion of privacy.
- Transmit pornography or other inappropriate material.
- Disclose information that is confidential to Archetype Group.

6.3 Format

The format of emails will be set up by the IT Manager and shall not be modified. Colour and image background are prohibited. Each collaborator of Archetype has a professional email signature that follow the corporate format. This signature must be downloaded from Intranet and then configured in the mail client software. IT will provide support to employees who do not manage to upload their signature by themselves. This email signature must not be modified unless approved by the Management.

6.4 Personal use

Archetype acknowledges that emails may occasionally be used for personal topic but requires that such use is limited and stays in accordance with this policy. If an email is personal, the user should make it clear that the message is not being sent on behalf of Archetype Group.

6.5 Attachments

To avoid obstructing Internet bandwidth and overloading mailboxes, sending big attachments should be avoided when size is bigger than 5MB. To exchange files bigger than 5MB, employee can use his personal OneDrive or Intranet SendIt and eProject.

7. Internet

7.1 Personal use

The internet is primarily made available to the employees for work related purpose. Archetype acknowledges that the internet may occasionally be used for personal matters but requires such use to be limited and only in accordance with this policy. In all instances, personal use of internet is prohibited during working hours.

7.2 Access to unauthorized website

Archetype can monitor sites that users are accessing. This monitoring includes the date and time that website was visited, the duration of the visit and the volume of data transferred. Users should exercise discretion and only access sites relevant to Archetype business.
Users must not in any circumstances, including for personal use, access sites that are prohibited by this policy. Archetype reserves its right to cancel user privileges or block access to sites deemed to be inappropriate. Figures disclosing Internet usage per employee could be to the IT Regulation Committee in case of inappropriate use.

7.3 Prohibited use

Internet, whether being used for personal or business, cannot be used for:

- Accessing websites that could be offensive or inappropriate to other people. This would include sites of adult, sexual, racist or discriminatory nature.
- Downloading music, video or any licensed property.
- Downloading any programs, updates or other nonstandard software.
- Registering own business email address on any unauthorized site. All email registrations are to be approved by the Department Director.
- Using any P2P software.
- Playing any online or offline games.
- Watching videos not related to business tasks.

7.4 Blogging and social media

Blogging by employees, whether using Archetype's or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material when engaged in blogging. Employees shall not engage in any blogging that may harm or tarnish the image, reputation or goodwill of Archetype or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging. Employees may also not attribute personal statements, opinions or beliefs to Archetype when engaged in blogging. If an employee is expressing his or her beliefs and opinions in blogs or social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Archetype. Employees assume any and all risk associated with their opinion.

8. Instant Messenger

The Instant Messenger such as Facebook Messenger, WhatsApp, Zalo, Yahoo, etc. are prohibited on all Archetype computers. The only authorized Instant Messenger are Skype, Skype for Business and Microsoft Teams.
All prohibited uses set for email use are also valid for instant messaging. Skype should only be used for instant messages or phone conversations. Any transfer of file must be done using emails, SendIt or any document management system already in place for projects.

9. Intranet

The access to Intranet is granted to all employees in Archetype. Different kinds of access have been defined in the system according to the employee position.

10. Authority and Responsibility

The IT systems and assets provided by Archetype are intended for Archetype business use exclusively. It is strictly forbidden to make use of Archetype's equipment for the creation or development of any personal project.
Employees have no expectation of privacy in anything that they create, store, send or receive on all IT systems (email, hard drive, server...). If deemed necessary, their emails and their files on servers can be monitored without prior notification upon request of the IT Regulation Committee.
It is strictly forbidden to copy, send or transmit any document belonging to Archetype to any third party without the prior approval of the Manager in charge of the production of such a document. This applies for design and administrative documents, for current and archived projects.
If a document produced by Archetype must be sent to a third party, it shall be sent in a non-modifiable format only, except if expressly requested and authorized by the Manager (especially important for AutoCAD file).
All employees, collaborators and visitors are responsible for the use of IT equipment and services within Archetype in compliance with this policy. If there is evidence of non-compliance, the company reserves its right to take disciplinary actions, including immediate suspension or termination and/or legal action, in accordance with the prevailing Labour Code.
In addition, any employee or collaborator who does not follow this policy, particularly by accessing or sending inappropriate or offensive material, or by illegal behaviour (unlawful or under anti-discrimination legislation), may be dismissed for misconduct. This would be in addition to any other appropriate legal proceedings, in accordance with the prevailing Labour Code.
Unless authorized by the Management and for specific and restricted cases, data MUST be saved on the server, in the directory of the project they pertain.

I hereby acknowledge that I have read and understood the above policy and I agree to follow the guidelines described in this policy. I acknowledge that a serious or continuing violation of the above policy will lead to disciplinary actions.

Name, date and signature of the employee