IT Policies & Procedures

***

7.2 Information Security Policy

Date:	**10-Jun-22**
Version:	**3.2**
Owner:	**Sudhir Rana - IT Manager**

Document review	
Last Review date	18.06.2022
Reviewed Version	3.1
Proposed changes (list chapter no and short description of changes) Review Committee	Adding document Annual review records Review for GDPR alignment
Review Committee	Global Information Security team
Approval Authority/Committee	Head of Global Information Security team
Next Review Due Date	10.01.2023
Note: Records within this table will not generate a change in the version number.	

TABLE OF OF CONTENTS

1.0 Summary

Security is one of the most important operating goals of Acu SA included in its 4Ss Policy, together with Simplicity, Speed and Substance). This policy sets the Security governance framework for Acu SA Users.

Acu SA encourages responsible use of information technology resources, both hardware and software, and full compliance with relevant laws and best practices.

This IT policy and procedure is reviewed annually and is part of the Acu SA Book of Policies & Procedures and can be found on the Acu SA Global Intranet site. It is to be read in conjunction with:

- Acu SA Green Book, the Acu SA Professional Code of Conduct which is distributed to all Acu SA employees;
- The other IT Policies & Procedures, in particular; IT.1 - Information Management.
- The Acu SA Privacy Policy

2.0 Purpose and Scope

2.1 Objectives

The purpose of this policy is to outline the acceptable use, usage and requirements of all individuals in the employ of Acu SA in regards to the computing infrastructure. The policy is in place to protect the employees and Acu SA. Inappropriate use exposes Acu SA to risks including virus attacks, compromise of network systems and services, and legal liabilities.

2.2 Core principles

Acu SA employees must use Acu SA technology equipment being aware of this policy. They must be aware of the importance of IT security aspects, take good care of the confidentiality of clients, respondents and Acu SA' Information and protect Acu SA' IT assets as if it was their own.

2.3 Scope

This policy is covering the following information security controls:

- Computer Acceptable Use
- Social Media
- Office 365 Usage
- Remote Access
- Mobile Device Use
- Password/Authentication
- Physical Security

2.4 Applicability

The policy requirements contained in this document are applicable to all divisions of Acu SA worldwide, including wholly owned subsidiaries and joint ventures in which Acu SA has a controlling interest or management responsibility.

This scope of this policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, free lancers, trainees, parttime and fixed-term employees, casual staff, interns and volunteers (collectively referred to as employees or users in this policy).

3.0 Responsibilities

3.1 Communication and Maintenance Responsibilities

Responsibility	Person responsible
Maintaining the policy	Global CIO, Global Information Security Director and General Counsel
Implementation of the policy at the country level	Country Manager and BU Managers
Communication of the policy within the BU	IT Services directors
Organizing appropriate training in order to comply with the policy	IT Services directors with HR support

3.2 Users' responsibility

Each User in the Group is responsible of appropriate use and performance of controls in compliance with the guidelines set out in this policy.

3.3 Violations

Violation of this policy may result in disciplinary action. This may include termination for breach of employment contract in the case of employees and temporaries; termination for breach of services agreement in the case of contractors (ex: consultants) and dismissal for interns and volunteers.

4.0 Computer Acceptable Use

4.1 Use of ACU SA Devices

Employees are expected to use company provided and approved internet access, e-mail, cloud service providers and services, computers, mobile devices (cell/mobile phone, tablet etc.), electronic media (disk, hard disk, CD-ROM, DVD, USB Data Keys etc.) and voice and voicemail systems for business purposes. Users are permitted access to the Internet and electronic communication systems to assist in the performance of their jobs.

Personal use means use that is not job/ Acu SA business related. Subject to any local deviations,, incidental and occasional personal use of Acu SA' internet access or electronic communications is permitted.

Personal use is prohibited if it:

- Directly or indirectly relates to personal business (i.e. all activities, non-job/business related, by which you can obtain a personal gain/benefit);
- Interferes with the user's productivity or work performance, or with that of any other employee;
- Adversely affects the efficient operation or attempting to find weaknesses of Acu SA' computer systems, networks or the desktop/laptop software;

Because access to such systems is considered a privilege of employment and the systems remain Acu SA property at all times, these systems could be subject to inspection from time to time by Acu SA (when legally permissible) to ensure compliance with this policy and to help ensure the security and protection of our business information.

Acu SA reserves the right to remove any non-business files or programs stored on company devices or to remove a user's access or use to Acu SA's systems.

Certain activities are prohibited when using the Internet or e-mail. These include, but are not limited to:

- Accessing, downloading, printing or storing information with sexually explicit content;
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages, files or images;
- Installing or downloading computer software, hardware, programs, or executable files unless reviewed by the user's local IT Services director and approved by Region IT Services director, with consultation of President Global IT Services & Global Head of Information Security;
- Installing, downloading, or providing for download by others, any content where copyright law is being violated
- Sending e-mail using another's identify, an assumed name or anonymously.
- Using the company allocated email address to register with non - business web sites or other non-business activity that aggravates the reception of spam mail.

4.2 Use of Personal Devices

Acu SA, through client contractual obligations, is mandated to store project related data on Acu SA owned and controlled services, servers, computers and mobile devices. As a consequence, Acu SA does not carry a BYOD (Bring Your Own Device) policy for its employees.

Personally owned devices such as PC's, laptops, tablets and smartphones are not permitted to be connected to the Acu SA network and/or are prohibited from storing any and all Acu SA or Acu SA client data.

Applications for exceptions are reviewed once a contract governing the use of the device has been signed and a business case submitted justifying it.

How to Apply:

A contract governing the use of those personal mobile devices such as tablets and smartphones - Non-Company Owned Personal Mobile Device Usage Agreement, is available from the IT Service Desk. The usage contract and business case must be submitted as an attachment inside of a Service Desk ticket.

The application will be reviewed by the local IT Services and approved by Regional IT Services Director for the respective region with consultation to the President Global IT Service and Global Head of Information Security .

It is also prohibited to use a personal e-mail address and system in performing work for Acu SA. The only authorized e-mail address is "FirstName.LastName@acuag.ch".

4.3 Authorized Software and Applications

All applications (for servers, PC, Cloud) and 3rdparty vendors must undergo the Global Vendor Assessment process and be approved for the specific scope of the project. This process can be initiated by addressing a vendor onboarding request to the Global PMO. The vendor onboarding request will assess the security, privacy and IT suitability of the proposed application and vendor. Once the assessment process is completed, the approval request will be submitted through the Acu SA Tech Investment Committee and will be processed by the Group Legal Department in charge of implementing contracts with vendors. No softwares or applications can be used without a formal contract signed-off by the Group Legal Department.

5.0 Social Media

Use of online social networking has become commonplace in our lives and is a convenient way to communicate, collaborate, share ideas, brainstorm and socialize.

This section provides guidance for the use of social media, which should be broadly understood to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other similar sites and services that permit users to share information with others. Facebook, LinkedIn, Twitter, Yammer, Skype, Lync Instant Messaging, blogs and social networking portals within business and academic environments our a few examples.

Due to its nature, the use of social media and blogs can expose Acu SA information to unintended targets.
Note: this social media section also holds true for the use of traditional media.

The following must be abided by employees at all times when using social media:

5.1 Personal Usage of Social Media

- Employees must make it clear in their social media profile that their tweets/posts are personal and do not reflect the views and opinions of Acu SA;
- Do not disclose, publish, post or release any Acu SA internal and/or confidential information, personal data, including PII, PHI and SPI;
- Disclosing information relating to Acu SA' clients to social media sites, blogs, wikis, online posting is strictly prohibited;
- If employees encounter a situation while using social media that threaten to become antagonistic, employees should disengage from the dialogue in a polite manner;
- Seek appropriate permission before users refer to or post images of current or former employees, members, vendors or suppliers;
- Employees must get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property;
- Do not publish anything that might be seen as representing ACU SA's position, view or opinion, without appropriate approval.
- Employees must show proper consideration for topics that may be considered objectionable or inflammatory, such as politics;
- Do not post fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages, files, images or anything that can create a hostile work environment;
- Social media use should not interfere with an employee's responsibilities or productivity;
- Follow good security practices and do not share passwords with anyone.

5.2 Business Use of Social Media

- AcuSA, client or names, logos or trademarks must not be used without written agreement from the relevant intellectual property owner. Employees are contractually obliged to maintain the confidentiality of client and respondent information as well as the information of any third parties with whom we have signed non-disclosure agreements; ·
- In relation with suppliers, Acu SA policy is neither to use publicly their names nor to allow them to use the Acu SA name, without their prior written consent for Group Legal Department;
- Where approval to cite or reference clients or partners is granted, employees must ensure the information published is fair, accurate and will not allow inferences to be drawn which could embarrass or damage the client/partner;
- Where content represents research findings, the publication of that content must be in line with Acu SA' procedures to publish polls;
- When using social media for market research purposes, the following must be abided by:
    - The Acu SA researcher must abide by the social media providers Terms and Conditions

- The rights of respondents that we uphold in conventional market research (online,

f2f, CATI) must be upheld when conducting research on social media ·

- Any published content must accurately represent Acu SA' position, strategy or Opinion and should be reviewed and approved in advance by the relevant business unit leader.
- Employees must show proper consideration for topics that may be considered objectionable or inflammatory, such as politics;
- Do not post fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages, files, images or anything that can create a hostile work environment;
- Do not disclose, publish, post or release any Acu SA internal and/or confidential information, personal data, including PII, PHI and SPI;
- Disclosing information relating to Acu SA' clients to social media sites, blogs, wikis, online posting is strictly prohibited;
- If employees encounter a situation while using social media that threaten to become antagonistic, employees should disengage from the dialogue in a polite manner;
- Seek appropriate permission before users refer to or post images of current or former employees, members, vendors or suppliers;

6.0 My I-365 Usage

The My I-365 platform is based on Microsoft Office 365 which provides best in class productivity, collaboration, communication, reliability and availability. The use of the various applications provided by Office 365, if not properly used or managed, could result in liability or loss of data to Acu SA. A fully patched and up to date version of Internet Explorer is required for proper and secure use of all Office 365 applications. The use of all other cloud collaboration suites (such as Google, Dropbox, etc.) is prohibited unless reviewed/assessed and explicitly approved by Group Legal Department. Employees must be abiding by the following at all times when using the following My I-365 modules:

6.1 My I-365 Usage

Outlook provides ACU SA's e-mail application as well as calendar, task and contact manager. It is important to take note of the following:

- The only authorized e-mail address is FirstName.LastName@acuag.ch or other XXX@acuag.ch shared mailboxes;
- Employees cannot send e-mail using another's identify, an assumed name or anonymously;
- Their electronic business cards must follow approved standards by Group Corporate Communications Department and their official title in iTalent;
- Employees cannot use the company allocated email address to register with non business web sites or other non-business activity that aggravates the reception of spam mail;
- Employees cannot forward business related e-mails to personal accounts or set up a rule to auto-forward all e-mails to non- Acu SA e-mail accounts; forwarding e-mails of a personal nature from Acu SA to a personal account is permissible;

- Data in e-mail (e-mails, attachments in e-mails, meeting invites, reminders, tasks, calendar events) are considered transitory data and cannot be permanently stored using Outlook;
- It is the responsibility of all users to store the data received in e-mail in the appropriate and applicable systems where long-term storage is provided for;
- E-mail services will not be used to send Acu SA /client confidential data and Personal data, including PHI and SPI;
- Users will not be able to create off line e-mail archives - PST files. In light of the above, it is important for users to understand that:
- E-mail (e-mails, attachments in e-mails, meeting invites, reminders, tasks, calendar events) is retained for 12 months in a user's mailbox (this includes the Inbox, Sent Items, Conversation History and all folders that are not archives) and then expunged;
- E-mail that is moved to the archives will be retained for 7 years and then expunged;
- The complete e-mail retention policy can be found in the "The Book of Policies and Procedures - IT.1 - Information Management".

6.2 I-365 – YAMMER

The My I-365 Yammer instance Provides a social networking platform for Acu SA employees to communicate, collaborate, share ideas, brainstorm and socialize. The use of Yammer must follow the same requirements outlined in Social Media Section at 5.2 of this document. In addition, the following important points must be taken in account by all users of Yammer:

- Yammer must not be used for permanent storage of data;
- There can be no posting of Acu SA /Client confidential information, personal data, including PHI and SPI;
- All posts older than 3 years of age or older will be deleted permanently. This will be reviewed and potentially revised later at Acu SA's discretion;
- Posts, notes and files will be removed from Yammer if they are in violation of the Social Media requirements as outlined in Section 5.0 of this document;
- Social Media spaces created by Acu SA staff are restricted to Acu SA e-mail domains. In cases where Social Media spaces need to be built for client deliverables, contact Acu SA IT.

6.3 My I-365 - Skype for Business (Formerly Lync)

Microsoft Lync is a multi-functional application that allows for instant messaging, , web conferencing, voice and video call between Acu SA employees. Employees must be abiding by the following at all times when using Lync:

· The use of instant messenger in Lync must adhere to the Social Media requirements in section 5.0 of this policy;

· Lync messages generated in instant messenger can be stored inside of Outlook in the Conversations folder. The messages in this folder are deleted as per the E-mail Retention Policy after 12 months.

· When initializing a web conference, to protect a user's privacy only the intended application should be shared and not the desktop as this will share all applications and desktop.

· The transferring of Acu SA /Client confidential information and personal data, including PHI and SPI using Lync is prohibited. The ability to transfer files is not permitted inside of Skype for Business

6.4 OneDrive

The MS OneDrive instance at Acu SA is a storage facility to be used as a collaborative space for non-personal data, including PHI and SPA. User files and presentations, SoW, MSA, RFP, bids, reports for which a collaboration space would be needed, can be part I go down down stored in OneDrive. Some important points to take notice of and rules to abide by:

- Files, upon creation or storage can only be read by the owner;
- Rights to the file and who they are shared with will be determined by the asset owner;
- Sharing is only with internal Acu SA staff;
- Acu SA/Client confidential information, personal data, including PHI and SPI may not be stored on OneDrive.
- Deleted files in OneDrive are moved to the Recycle Bin where they are kept for 90 days after which point they are deleted permanently.
- Security settings for OneDrive are set to insure an optimum level of security and protection for user files, and no attempt to change settings should be made. For compliance, application logging/auditing of all Acu SA employees' OneDrive settings and activities are regularly performed - employees found to be changing their security level, storing personal data on OneDrive or otherwise in breach of Acu SA's security policies face disciplinary action, up to and including dismissal.

6.5 SharePoint

The Microsoft SharePoint instance at Acu SA is centrally managed and used to store and share files.

It is the only approved solution to share knowledge within the Group and is the technology behind the Global Intranet site (accessible to All Staff for some parts).

Access to some other SharePoint portals is given on a need to know basis.

The storage of personal data, including PHI or SPI is not permitted on Office 365 SharePoint sites.

- Storage of client data is permitted, but due to client residency requirements, it is the responsibility of the user to obtain the written consent of the client before doing so, where such requirements exist.

- Information deleted on a SharePoint site will remain in the Deleted Items for 90 days, after which it will be permanently deleted.

- All new requests for access to a SharePoint site must be submitted by the SharePoint site owner via the Acu SA self-service portal.

6.6 New Microsoft Offerings

Microsoft is releasing new products periodically to the O365 suite. The following must be observed for all new offerings:

Before release or usage of the application, it must undergo an Information Security and Privacy Impact Assessment

6.7 Powe BI

Power BI is a suite of business analytics tools to analyze data and share insights.

- The processing of personal data, including SPI or PHI, is not allowed using Power BI.
- Uploading data sets to Power BI could result in personal data, including SPI or PHI, being uploaded to the cloud - it is absolutely critical that all data sets are inspected before being uploaded to Power BI. It is the responsibility of the user to check and verify no personal data, including SPI or PHI, is being uploaded.
- Power BI should not be used to process and share MIS data (iTalent, Symphony etc) as there BI is made for this.

7.0 Access Policy

Access rights to Acu SA information and/or IT environment will be granted based on the need to work and need to know principle and Acu SA Access Management Policy. Access rights will be requested by the line manager and approved/rejected by the asset owner.

7.1 Unauthorized access

Employees are not authorised to have access to confidential information and personal data, including PH and SPI, related to clients or projects they are not working on and do not have a need to know, nor should they discuss confidential information or personal data, including PH and SPI, with other Acu SA employees who are not working on matters for the same client.

They must not try to gain access to any confidential information all personal data if they are not related to a legitimate specific business need.

The management of the access to Acu SA systems is centrally managed by Acu SA Tech teams responsible for each application. For MIS and e-mails, they are managed by the Global Access Management team.

7.2 Remote Access Policy

All Acu SA staff must use an Acu SA imaged device and connect to one of the remote access hubs on the Acu SA network for access.

All remote connections to Acu SA IT environment must be connected by creating a VPN (Virtual Private Network) tunnel to one of our remote access hubs.

- All staff must be Acu SA employees with user IDs in Acu SA' active directory.
- All connecting devices (laptop, desktops) must be imaged by Acu SA.
- When a user is connected to the VPN, all network and Internet traffic must go through the Acu SA network by default. Simultaneous, separate connections to the Internet are not permitted.

8.0 Mobile Device Use

8.1 Scope

This section applies

- to all Acu SA owned or controlled "mobile devices", which includes
  - Tablets
  - Smartphones
  - Cellphones
  - PDAs
  - Small Computing Devices; and

- All uses by Acu SA employees in the performance of their duties when using an Acu SA owned or controlled mobile device:

  - In the course of work for data collection, such as face to face interviewing, by when performed by Acu SA staff and contractors collectively known as "Iinterviewers; access for data collection purposes is restricted to only the applicable data collection program.

  - Aca SA e-mail and data access for all users .

8.2 Out of Scope

For CD's, DVD's, portable hard drive, USB key and hard disk please see section 13.3 of the Information Management Policy.

8.3 Configuration

- In the case of data collectiontablets, Acu SA corporate e-mail is not permitted to be accessible for "Interviewers" in the course of their data collection work.

- Devices must be password protected; passwords must be 6 or more characters in length. A biometric authentication (such as a fingerprint) can be used in lieu of a password on devices where the capability exists,

- The mobile password must be changed every 6 months.

- In the case of devices managed by Microsoft ActiveSync, password complexity must be enabled.

- The maximum time, in minutes, that elapses before the mobile device locks and prompts the user for the security password: 15 minutes.

- All Acu SA owned or controlled mobile devices must have the ability to be remotely wiped.

- All Acu SA owned or controlled mobile devices used in the role of data collection or Storing internal or confidential information must have their storage devices encrypted (i.e.: supporting and deploying whole disk encryption) using 256-bit AES. For more information on information classification, encryption standards and encryption key management please see the Acu SA Information Management Policy.

8.4 Usage

Devices may only access Acu SA corporate e-mail through approved channels (e.g.: Outlook Mobile Access (OMA) Exchange Servers, ActiveSync); corporate e-mail may not be simply forwarded to a device.

Lost or stolen devices must be reported to Helpdesk immediately so the command can be sent to erase securely the data from the missing device. The steps for reporting are:

- To the local IT Service Desk
- To the Head of Global Information Security - it@acuag.ch
- On weekends and bank holidays +91 8291980820.
- Mobile devices must be safeguarded as per section 10.3 of this policy.
- The failure promptly to report such loss or unauthorized access may result in disciplinary action.

9.0 Password/Authentication

Access to Acu SA' environment will be controlled by means of user name and password and/or other authentication methods.

To enhance security environment, Acu SA has established a password policy defining the password length, complexity, reuse of old passwords and frequency of password change.

9.1 Password Length

The password must be at least eight (8) characters long.

9.2 Password complexity

The password must use a combination of lowercase, uppercase, numbers and nonalphanumeric characters ("special characters") so the password cannot easily be guessed by someone trying to break in.

Note: See below for the rules that must be followed to ensure the password meets minimum requirements.

9.3 Password Re-Us

A password cannot be re-used until after it has been changed to a different password 3 times. If the default frequency of 3 months between changes is used, the earliest it can be re-used is after almost a year, but it is recommended not re-use them at all.

9.4 Frequency of Change

The password must be changed at least every 3 months (90 days). If a user connects to the network on a wired connection, he/she will be prompted to change the password starting 21 days before expiry, however, those who connect remotely, or who always use wireless, will NOT be prompted. In that case, please set a recurring task in Outlook as a reminder to change the password before it expires to prevent being locked out.

9.5 Confidentiality of Authentication Details

The authentication details (*ex: user name, password, token or other authentication means*) are to be considered private, and should not be shared with anyone, whether Acu SA employee or non-employee. Each user is responsible for all activity occurring under his/her account, regardless of who was actually at the keyboard. Unauthorized disclosure/loss of the authentication details must be reported to the local IT in a timely manner, requesting the change of the authentication details.

To further protect the user account any device must be locked (ex: For Windows based devices press Ctrl-Alt-Del and choose Lock Computer) when the user has leave the system logged on and unattended.

If a user needs access to a resource for which no current permission exists, the user must call the helpdesk to have access granted; a user may not use someone else's account. Password sharing is strictly prohibited. Additionally, all accounts must accurately identify the user.

10.0 Physical Security

10.1 Clean Desk and Clear Screen

A clear desk and clear screen approach is used to reduce the risks of unauthorized access to, or loss of, or damage to, information. Users have to ensure that:

- at any time, unattended working areas are kept clear of all media including, but not limited to paper, DVD, tapes, flash storage, or any other media that may contain security sensitive data as defined by Acu SA data classification standards all personal data.

- Employee work areas, like cubicles and offices are kept clean and organized, and that all media, regardless of its classification, our not present on work surfaces, desks, bookshelves, or unlocked cabinetry if the employee is not present.

- appropriate facilities in the office in which media can be stored and locked away our used, including in lockable closets, filing cabinets and cupboards.

- Personal computers, computer terminals, tablets, and smartphone our locked (ex: for Windows Ctl+Alt+Del - Enter or + L) when not in use, and turned off at the end of the working day. Laptops should be locked with a cable lock during business hours, and orkept in a locked cabinet when stored in the office overnight.

- Vacated offices and cubicles, which do not currently have a purpose or staff resident need to have all network jacks disabled. This can be achieved by disconnecting the jack from the local switch providing connection to the Acu SA network.

- It is mandatory to use a password protected screen saver that automatically engages after 15 minutes of inactivity.

- Incoming and outgoing mail collection points should be protected or supervised so that letters cannot be stolen or lost, and faxes should be protected when not in use.

- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

- Confidential papers are to be disposed off by using shredders or designated shredding bins. Note that documents that are thrown into the general rubbisg/trash become part of the public domain. Anyone can look through Acu SA's rubbisg/garbage once it has left our control.

10.2 Physical Access

- No person should be allowed into Acu SA premises that is unknown. This is the most common way to breach physical security;

- Anyone who is attempting to gain access to Acu SA premises needs to be challenged to produce their swipe card or Acu SA ID;

- Visitors/3rdparty service providers (non Acu SA personnel) need to be accompanied at all times when in Acu SA offices;

- Visitors and 3rdparties must log in and out of Acu SA offices; visitor log records shall be maintained for a minimum of 2 years;

- No unknown and unidentified people must be granted access to Acu SA offices or processing facilities based on good faith;

- Access cards should not be lend to other staff or persons.

10.3 Requirements for Safeguarding Laptops, PCs and Mobile Devices

Acu SA employs various standards to protect information on computers and laptops but users must be mindful of the following:

- The information on a lost or stolen laptop, PC, mobile device or USB thumb drive that is not encrypted can still be accessed and read.

- The BIOS password and Windows login password are key to security but can be defeated with time and various utilities.

The following should be incorporated into any user's routine:

- files stored on a laptop should be backed up to the file server on a regular basis.

- files should be transferred of off a laptop when they are no longer required.

- No data classified as either internal or confidential must be stored on a laptop, mobile device or USB drive, unless media encryption has been enabled. Any device such as a laptop, mobile device or USB drive must be encrypted with whole disk encryption. If this data is stored on a device, the user must ask the IT department to install whole disk encryption.

- Secure any laptop with a cable lock, even during working hours.

- Laptops need to be secured with a cable lockin a drawer or filing cabinet when not in use or not taken home.

- Never leave a laptop in a vehicle where it is visible. It should be locked in the secured trunk/boot . An SUV, Pick-up, Van, Mini-Van or Hatchback's storage compartment is not a trunk/boot.

- Not all car trunks/boots can be properly secured. A properly secured car trunk/boot must have a trunk/boot pop latch that can be locked and rear seats that can be locked into place preventing access to the trunk/boot.

- In a hotel, the laptop must be locked in the room safe (if it is available) or stored out of sight when the user is not in the room.

- Airports, train terminals, subway stations, bars are prime areas for laptop theft. Laptop bags need to be kept near and never be left unattended. Mobile devices should be kept on the user and control. When a laptop bag is not over the user's shoulder, it must be kept in sight, and preferably one of the laptop bag straps is looped round an arm or leg.

Appendix 1 - Definitions and Abbreviations

Personal Data	Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, biometric data an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; PII and personal data are synonymous, PHI, and SPI are forms of personal data
Protected Health Information (PHI)	*This is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.*
Personally Identifiable Information (PII)	This is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
Sensitive Personal Information (SPI)	This includes data about an individual's racial or ethnic origin, age, Personal date of birth, political opinions, religious beliefs (or other beliefs of a similar nature), physical or mental health, sexual life/sexuality, financial information (bank account number, credit scores, income, salary, bonus, Acu SA employees financial data, etc) and criminal proceedings or convictions.
Intellectual Property (IP)	*Intellectual Property includes (without being limited to) all present and future proprietary rights, licenses, title and interest in any intellectual property rights including industrial property rights, trademarks (registered or unregistered), rights in invention, service marks, patents, copyrights, design rights, database rights registered, designs and know-how, algorithms, APIs, databases, diagrams, formulae, inventions (whether or not patentable), configurations and architectures, processes and workflows, proprietary information, protocols, specifications, software code programs languages and codes rights (in any form, including source code, and executable or object code), subroutines, techniques, user interfaces, URLs (whether or not embodied in any tangible form and including all tangible embodiments of the foregoing, such as instruction manuals, prototypes, notebooks, samples, studies and summaries), proposals to clients, products, questionnaires, lay-out and design of reports and portals.*
User	An individual accessing Acu SA physical offices, data and IT *Infrastructure that contains Acu SA data in it various forms. This user can be an employee, contractor or 3rd party vendor.*