Information Security Acceptable Use Policy

CP Axtra Group sets out the minimum requirements for the acceptable and appropriate use of CP Axtra Group's Information Resources by all CP Axtra Group employees, contractors and third party users (CP Axtra Group Personnel). All CP Axtra Group Personnel must adhere to the policies included in this standard unless prohibited by local laws or regulations.

This standard applies to all computing and communication resources, including but not limited to cellular phones, smart phones, tablets, desktop workstations, laptops, network servers, optical storage media, stand-alone systems, single or multi-user systems, telephone and voice mail systems, voice and/or video over Internet Protocol (VoIP), systems connected to any CP Axtra Group network or any other computing or communications system owned, operated or administered by or on behalf of CP Axtra Group.

1. Ethical usage of resources

1.1 CP Axtra Group characterizes the following behaviors as unethical and therefore unacceptable:

a) Any activity which purposely seeks to gain unauthorized access to any resources,

b) Disrupts the intended use of the resources,

c) Wastes resources (people, capacity, computer) through such actions,

d) Destroys the integrity of computer-based information, and/or

e) Compromises the privacy of other users including customer information, supplier information or employee information etc.

2. Information security responsibilities

2.1 You must read, understand and always comply with all information security policies.

2.2 You must consult your reporting manager, or the information security department to clarify any doubts pertaining to these policies.

2.3 You must report the following to your line management or to information security department:

a) Suspected or actual security incidents,

b) Security weaknesses in people, processes and/or systems,

c) Security risks, and/or

d) Security issues

2.4 You must not tamper with various security controls implemented within the company.

2.5 You must always comply with the Non-Disclosure Agreements (NDA) even after employment with CP Axtra Group has been terminated.

2.6 You must always comply with the personal data protection policy and data security policy. In case there are the personally identifiable information (PII) breach or confidential company information breach. You, data owner or system owner must immediately inform DPO department and information security department.

3. Usage of assets

3.1 Company Asset(s) shall be defined as a system, network, desktop, internet, email, account, configuration and any documents belong to CP Axtra Group as following responsibilities:

System and Network Activities

- The following activities are strictly prohibited, with no exceptions: Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
- Revealing your account password to others or allowing use of your account by others.
- Effecting security breaches or disruptions to network communications.
- Port scanning or security scanning except by authorized personnel or contractors.
- Executing any form of network monitoring which will intercept data not intended for the employee's use, unless this activity is a part of the employee's normal duty.
- Circumventing user authentication or security of any host, network or account.
- Launching attacks on other computers or networks (e.g. denial of service attacks).
- Using any code, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the network.
- Providing information about, or lists of, employees to outside parties.
- Providing information about the CP Axtra Group's systems or security precautions to unauthorized parties inside or outside the company.

Remote access

- Remote access right shall be granted based on least privilege principle. The access right shall be terminated immediately after resignation, end of contract or end of project.
- Any method of remote access from the internet network (VPN, SSH etc.) must be approved by information security department and shall be renewed every 3 months.
- Using unauthorized remote access software/method is prohibited.
- While joining to the internal network, Other users are prohibited to access the computer.

Computer usage

- Users are responsible for the security of their computers and should take adequate measures to restrict physical and logical access to their desktops.
- Users should not change any hardware configurations, settings in operating system or any applications installed on their desktops. If users require any change in hardware (For e.g. attaching a CD-ROM drive or USB drives / access or increase system memory) or software settings, they should contact the respective managers and seek the approval along with business reason to do so.
- All the systems will have administrative rights disabled. Any requirement should be supported with a business reason and approval from the manager of the respective team.
- Users are prohibited from bridging the internal network. Directly accessing external networks via personal VPNs, cellular phone tethering, external Wi-Fi access points, etc. is strictly prohibited.

To prevent the risk of unauthorized access, users should adopt the following measures:

- Log out of all applications or turn off the desktop if you are leaving your desktop unattended for an extended period of time.
- While desktop is unattended for short durations, enable the screen saver with password protection.
- Do not enable sharing of folders in your computer with other users over the network.

Internet usage

- Internet access is provided to users for the performance and fulfillment of job responsibilities.
- Occasional and reasonable personal use of Internet services is permitted, provided that this does not interfere with work performance.
- All access to the internet will be authenticated and will be restricted to business related sites. CP Axtra Group will have the right to filter and prohibit access to certain websites at its own discretion.
- Users should not use Internet facilities to:
  - Download or distribute malicious software or tools or to deliberately propagate any virus.
  - Violate any copyright or license agreement by downloading or distributing protected material.
  - Upload files, software or data belonging to CP Axtra Group to any internet site without authorization of the owner of the file / software / data.
  - Share any confidential or sensitive information of CP Axtra Group with any internet site unless authorized by superior/ controller.
  - Post views or opinion on behalf of CP Axtra Group unless authorized by top management.
  - Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting CP Axtra Group.

Email usage

- Users are prohibited from sending or forwarding emails with CP Axtra Group confidential information, such as customer information, business strategy, etc., without legitimate justification and required approval outside CP Axtra Group
- Users are prohibited from sending or forwarding following categories of emails within or outside CP Axtra Group:
  - Emails with any libelous, defamatory, offensive, racist or obscene remarks.
  - Emails that contain viruses or worms.
  - Chain mail containing virus hoaxes, jokes, political advocacy efforts, religious efforts and others.
  - Emails containing any document, software that protected by copyright, privacy or disclosure regulation.

3.2 All Asset(s) must be returned promptly after its intended use is over or the employment has been terminated.

4. Identity protection

4.1 CP Axtra Group issued authentication credentials (including hard or soft tokens) must be kept as a secret. These secrets shall not be shared with anyone else.

4.2 The authentication secrets such as passwords/ PINS shall not be scribbled in places where others are able to see and follow the password construction below:

Password construction

Users should choose passwords that are easy to remember but difficult to guess. Some of the guidelines for password constructions are:

- Do not use own name, short form of own name, own initials, names of family, friends, co-workers, company or popular characters.
- Do not use personal information like date-of-birth, address, telephone numbers etc.
- Do not use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Do not use any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- Strong passwords have a minimum length 8 characters and can be constructed through a mix of numerals (1,2,3), special characters (!,@,#,$) and capital letters / small letter (A,B,c).

To prevent the risk of unauthorized access:

- Users should ensure that nobody is watching when they are entering password into the system.
- Users should also not ask others (including customers and colleagues) for their passwords.
- Users must change their passwords under any of the following circumstances:
  - At least once in 90 days.
  - As enforced by system (applications and operating system)
  - As soon as possible, after a password has been compromised or after you suspect that a password has been compromised.

4.3 The system that requires to connect with third party tool. The third parties' tool must approval by information security department.

5. Privilege misuse

5.1 Any privileges thus granted shall not be misused.

5.2 Users must report any additional privileges that are given promptly to the respective business owners and/or custodians of such systems.

6. Bring your own device policy

6.1 Users must acknowledge this Information Security Acceptable Use Policy before connect bring your own devices to CP Axtra Group's workplace or connect to CP Axtra Group's email

6.2 CP Axtra Group shall have the right to control company data on bring your own devices for company data protection and security purposes only.

6.3 CP Axtra Group shall have the right to remote wipe or delete the company data on bring your own devices under following situations if it is used for data storage:

a) The bring your own devices is lost, or

b) If the employment contract has been terminated.

7. Social media, blogs, forums, file shares, etc.

7.1 Unless authorized staff shall not engage in social media interactions for the company. You must not violate the intellectual property rights of CP Axtra Group and of others.

7.2 Staff shall not post company information or their own private opinions about the company in social media.

8. Compliance

8.1 The employees and relevant third parties shall acknowledge the acceptance of this form by signing a page at the end of this document or acknowledgement via HR system.

8.2 Compliance to these policies is mandatory. Any violation of the acceptable use policies will result in disciplinary action.

8.3 Lack of understanding of these policies is not an excuse for violating them.

9. Disciplinary actions

9.1 Violation of established policies (including information security policies) will result in disciplinary actions, which may be initiated by your line manager with due consultation from human resources department, compliance departments and/or information security department.

9.2 The disciplinary measures shall be appropriate and proportional to the violations occurred. It may range from forcing the staff to repeat the security awareness training to termination of employment.