ASTRA GROUP

INFORMATION TECHNOLOGY

COMMUNICATION & INFORMATION SYSTEM

User Agreement

IT-ACCEPTABLE USE POLICY

CREATION DATE: MAY 09, 2022

VERSION: V.3.2

Document Control

Change Record

Date	Author	Position	Version	Change Reference
15-MAY-16	Mohammed Khasawneh	Group IT Manager	1.0	No Previous Document
5-DEC-16	Mohammed Khasawneh	Group IT Manager	2.0	1.0
5-FEB-17	Mohammed Khasawneh	Group IT Manager	3.0	2.0
30-JUL-19	Information Technology	Head office	3.1	3.0
09-MAY-22	Information Technology	Head office	3.2	3.1

Reviewers

Name	Position
Mohammed Khasawneh	Group IT Manager
Shahzad Ahmad	Head of Technology Infrastructure

Abstract

To obtain signed agreement from all personnel signifying understanding and acceptance of applicable communications & information systems policy, legal requirements concerning the use of information systems and access to network resources within Astra Group (AG). This policy applies to all staff, trainees and partners.

All AG Employees MUST sign a copy of this policy. This agreement should also be provided to any new employee before commencing to work.

Purpose

The purpose of this document is to outline user responsibilities and acceptable use to promote efficient, legal and ethical use of Astra Group Communications and Information systems and to maintain confidentiality of data, files, assets and networks as well as protect the proprietary rights of third parties for the commercial tools and software in Astra Group.

Communications and Information Systems User Agreement

Communications and Information Systems cover computing, data (including documents, other electronic files, e-mail and recorded voicemail messages), collaboration and communications facilities including (but are not limited to) Servers, desktop computers, laptops, tools, telephones, mobiles, photocopiers, software, e-mail systems, web services, Internal or external communications networks (Internet/Intranet) and any other resources that are directly or indirectly linked or accessed.

Communications and Information Systems and the information contained within these systems are Astra Group's Proprietary, if compromised, destroyed, disclosed or lost, could result in adverse consequences such as (but are not limited to) financial loss or disruption of business. Proprietary includes: customer, supplier and employee lists, financial information, such as costs, investments, earnings, sales and forecasts; sales and marketing strategies; wages, salaries and benefits; requests for proposal; personnel files, including compensation and employee records; business plans and strategic objectives, sales, service, recruiting and training plans.

Communications and Information Systems are intended for business purposes only, employees are permitted to use them only as necessary to fulfill job or assignment requirements with high level of care; personal use of these communication tools are permissible only within reasonable limits and at the sole discretion of Astra IT Management.

Astra Group reserves the right to monitor all aspects of its Communication and Information Systems at any time without notice, moreover a disciplinary action, ranging from revocation of access to dismissal may result from the failure to adhere to what contained in this document. The mentioned rules and conditions in this agreement apply to all individuals who use communication and information systems of Astra Group.

1. Classified Processing

- User shall not process classified information (can be designated top secret, secret or confidential) on any system which is not specifically approved and marked for the appropriate level.
- User shall report to the IT Manager any inadvertent or unapproved classified processing on non-classified systems.
- User shall not process or store classified information on privately owned (personal) computers or media without approval.

2. Credential Protection

- User shall always protect his/her passwords and authentication tokens from disclosure and loss.
- User should practice a difficult-to-guess password with a minimum of eight characters in length which consists of 3 of the 4 character sets (numerical characters, special characters, capital and lower-case letter).
- Predefined or default password should be changed immediately at first logon when assigned.
- Passwords should never be written down or shared with others.
- Previously used password should not be repeated, also password should not contain obvious personal data, (i.e., last name, mobile numbers, relative's names, pet's name, etc.).
- The user must change the password every three months.
- If password needs to be stored electronically, the user shall ensure that it is stored using encryption method.
- Same password should not be repeated in different systems including SSL-VPN connections to access company's internal network resources.

3. User Account(s)

- Sharing or disclosing user account with others is prohibited.
- User shall not attempt to access other user accounts or data that are not explicitly authorized to him/her.
- User is accountable for all actions taken under his/her credentials.
- User shall only use the domain associated with his/her user account provided by the system administrator.
- Those administrators having multiple accounts (either same or different username) in more than one domain of AG shall not use the same password for their user accounts.

4. Data Protection

- User shall treat storage media in accordance with the highest level of data protection and security, e.g., to protect against exposure to strong electromagnetic fields.
- While storing any information, user shall ensure that it is stored in a secure manner and reasonably protected from unauthorized access.
- User shall protect confidential data of the company and should not share it with any unauthorized individuals.
- There shall be a clear distinction between personal and business data and should be kept separately.
- The user is strictly prohibited from changing the protection settings that have been implemented by the IT department.
- The user shall take backup of the data periodically (preferably external drives).
- The user shall ensure their systems are locked (temporary out-of-office) or shutdown their devices while leaving their workplace (end of work).

5. Physical Security

- User shall not remove AG's information systems or software without expressed written permission of the Information Technology Manager.
- When laptops, mobile, PDAs, tablets or any portable devices are in user's possession outside Astra Group premises, user held responsible for providing physical security and keeping items under exclusive control. ***User held accountable for its lost or damage***.
- In case of theft or data loss, user held responsible to report that immediately to IT department. Always, user shall keep backup of important data (*Ref: 4. Data protection)*.
- All personally owned devices must be registered and approved by the IT department.
- Upon resignation or contract termination, User is responsible to return any company owned device(s) or computer system under his/her custody.

6. E-mail

- The e-mail system is provided solely for official business usage; accordingly, user shall not use it for personal matters or subscribe on different portals
- User shall keep his/her signature's information updated and matched with the HR system records.
- User shall limit his/her non-official use of the e-mail system to prevent interference with their official duties or cause degradation of network services.
- User shall not send e-mail that is malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable. Also, user shall report to IT staff upon receiving any related email instantly.
- User shall not generate, distribute, publish, or facilitate unsolicited mass email, promotions, advertisings, or other solicitations ("spam").

- User shall not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.

  Note: System administrator will never ask for your username and password, and the user should not respond to such e-mail requesting such kind of information.

7. Internet Use

- Accessing to public networks (i.e., the Internet) is solely for official business usage.
- User shall limit his/her non-official access to the Internet to prevent interference with any official duties or cause degradation of network services.
- User shall not access web sites or social media containing malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable text or graphics.

  Social media tools, web-based and mobile technologies, tools and platforms are effective ways of communicating with others on both a personal and professional level. However, it is essential that the use of social media is carefully considered in compliance with the above-mentioned rules to avoid the misuse of communication medium.
- When available technology fails to block undesirable Web sites, User should promptly report to IT staff about those sites that were unintentionally accessed.
- User shall abide by all internet security rules/polices implemented by the IT department and will never use any third-party applications establishing connections (e.g., VPN and Hotspot etc.) which may cause security breach.

8. Cloud Computing Services

- Reading this AUP, you acknowledge that the IT has no power to control the content of the information passing over the Internet and its applications, including e-mail; chat rooms; news groups etc.., and that the IT cannot be held responsible or liable, directly or indirectly, for any of the abovementioned content, in any way for any loss or damage of any kind incurred as a result of, or in connection with your use of, or reliance on, any such content.
- Confidential or Sensitive Data is NOT ALLOWED to be processed, created, collected, stored nor archived in the cloud UNLESS service is determined to support security controls as necessary to sufficiently protect the data.
- Users shall not use enterprise accounts of any of the cloud computing services for their personal use, also user shall be aware that the data shall never be shared to their personal emails or with any anonymous emails.
- While using, sharing, or storing data over the cloud, user shall be aware of the sensitivity of the data and information, and shall only be stored or shared within AG's cloud computing environment.
- User shall always make sure that the ULR's they are using in the browsers are legitimate and to avoid accessing the links using search engines or links received in email.
- User shall immediately report to IT Staff, if found any suspicious or unauthorized activity to their cloud account.

9. Network and Remote Access

- User that wishes to access the network using his/her **personally owned** devices may do so using only authorized software and only with the prior approval of the user's supervisor and the IT department.
- User shall not allow any connection to his/her machine or workplace network or system using TeamViewer, AnyDesk, Quick Assist or Windows Remote Desktop Access etc. for any reason without prior approval from Information Technology Manager.

10. Remote work

- User shall seek prior approval from his direct manager and IT Manager for the remote work by providing a justifiable reason.
- While using IT Asset for remote work user shall adhere with AG - Standard Cybersecurity Controls.
- User shall contact IT department for technical support while facing any IT related issues.
- Support shall be provided to the user through one of the remote access programs approved by the IT department such as (Team Viewer, AnyDesk and Quick Assist).
- The user is obliged to return the asset to the IT department and sign the Asset Return Form upon its delivery.

11. Antivirus System (Endpoint protection)

- AG has installed antivirus on each machine to protect against malicious threads. However, each user is responsible for taking appropriate measures to ensure that it is updated, and system is protected. These include ensuring that any files or data brought from outside is virus checked by the IT department before use. This includes virus checking of all external forms of media.
- User shall ensure that antivirus application is always running on their workstation and shall not be paused/stopped. In case it is found that the program is not running, user must inform IT department immediately.
- Any concerns regarding the source or content of any CDs, USB Flash Drives, or an email attachment should be referred to the System Administrator or IT Manager.
- In case there is any indication of a virus or any other security threat, User shall inform the System Administrator or IT Manager immediately.
- User should not change any settings for the protection system that have been installed by the IT department.

12. Printing

- Once printed, user shall not load the same paper for printing.
- User shall avoid using printers for personal printing.

- User shall not exceed the paper limit allocated by the printer to avoid paper jams.
- User shall not try to repair or change the printer components himself.
- User shall contact the IT department in case of any malfunction or change of inks.
- Before copying, user shall ensure that the paper is not stapled, as this might cause serious damage to the printer.

13. Copyright Protection

- User shall not download and/or install third party software without prior approval of the System Administrator. Also removing copyrighted/Licensed software from AG's equipment is prohibited.
- User is liable for any software copyright or license violations committed on AG systems under his/her control.
- Software and hardware licenses are the proprietary asset of AG. Therefore, it should not be used on private devices and/or shared with others.

ASTRA GROUP

INFORMATION TECHNOLOGY

COMMUNICATION & INFORMATION SYSTEM

User Agreement

IT-ACCEPTABLE USE POLICY

Using Astra Group's Communications and Information systems is restricted to authorized users only. Anyone who accesses this system without authorization or exceeds authorized access or violates the conditions of use of IT Facilities and resources could be subjected to disciplinary or legal actions, or both under Law.

By accessing Astra Group's systems & networks, you hereby agree to comply with the above Information Security requirements and consent to having your activities and access monitored by system software. If this monitoring reveals suspected unauthorized use or illegal activity, the evidence may be provided to supervisory personnel and legal authorities.

Date:	Employee Name:
Department:	Position:
Signature:	