IT Code of Conduct

Document No. POL-301
Rev. 4.1
Effective: 4/12/2023
Classification: Internal 3

Revision History

Revision #	Revision Date	Description of Revision	Authorized By	Author
1.0	6/9/2009	Initial version	Executive Management	Ann Heathcott
2.0	4/28/2015	Updated	Executive Management	Gary Watson
3.0	3/31/2022	Add personal device usage policy components, Employee WIFI and security changes for environment.	Executive Management	Ann Heathcott Legal Kelly Cruse
4.0	3/1/2023	Reviewed for updates and added IT to Service Desk for clarity.	Executive Management	Ann Heathcott
4.1	3/13/2024	Updated title, corrected policy number, and added reporting when unsure of security/privacy items.	Executive Management	Ann Heathcott

As a user of the Company's Information System (the "System"), which includes its computers and equipment, e-mail, Internet/intranet access through those computers/equipment, Employee WIFI and voicemail, I understand that:

1. ***General Policy***. The System is the property of and/or is provided for the benefit of the Company and is intended to be used primarily for the Company's business and business purposes. I am responsible for using the System in an effective, ethical, and lawful manner that complies with this Code of Conduct.

2. ***Access***. The User ID assigned to me, and passwords used by me, provide me the capability to access and use the System. Access may be approved with restrictions that limit the sites available to me and the type of service allowed. I am responsible for protecting the System by:

    a. Not knowingly sharing my User ID with or disclosing my passwords to another person.
    b. Only authorizing Multi-Factor Authentication ("MFA") requests when I have personally requested access to the System.
    c. Changing my password whenever I know or suspect that it has been disclosed to another person.
    d. Not using or attempting to use any other person's User ID or passwords to obtain access to the System.
    e. Only accessing data for which I have a specific authorization.
    f. Reporting security violations and suspected security violations that I observe or that otherwise come to my attention to the Atlas IT Service Desk, Chief Security Officer, or VP Information Technology.

3. ***Content Restrictions***. All communications and use of the System should be primarily for the Company's business and business purposes. I am responsible for:

    a. The content of all text, audio, or images (together referred to as "Messages") that I place on or send or forward over the System (including specifically e-mail, the Internet/intranet, and Employee WIFI).
    b. Ensuring that my use of the System, including Messages that I send, are not for my personal gain, including soliciting non-Company business or conducting commercial activities, or advancing my individual views, for which I will use my own name on another Internet/intranet or WIFI system.
    c. Ensuring that I do not use the System for any activity prohibited by law or Company policy.
    d. Not publishing, posting, sending, forwarding, or otherwise disclosing fraudulent or obscene Messages, including Messages with abusive, profane or offensive language, or Messages that are intended to intimidate, abuse, threaten, harass, or frighten a person and/or that would violate the Company's Anti-Harassment Policy prohibitions against unlawful harassment on the basis of race, color, national origin, religion, sex,

sexual orientation, gender, gender identity, age, pregnancy, physical or mental disability, or any other Locally Protected Class.

e. Using only my own name and not any assumed name to send Messages and not obscuring the origin of any Message.

f. Ensuring that materials that I obtain or transmit through the System do not infringe the property rights of others, including those arising under licenses and copyrights, and are not copyrighted materials belonging to other entities, although I may download one copy of copyrighted material for my own personal use.

g. Any security violation traceable to my User ID.

h. Ensuring that personal data will not be disclosed to any unauthorized person, either within the organization or externally.

i. Ensuring that my intermittent use of the System for personal purposes (i) is not inappropriate or excessive, (ii) does not result in expense or harm to the Company, (iii) does not have a negative security impact, and (iv) does not otherwise violate this Code of Conduct.

4. ***Personal Electronic Device Usage.*** Access to Company networks and/or Company data on an Employee's personal device must meet Company standards for data security. Utilizing a personal device for business purposes is voluntary. I understand and acknowledge that:

a. The personal device must be secured by a strong passcode or pin.

b. Employees must use MFA to access Company networks on a personal device.

c. Only Company-approved applications may be used to access Company networks and/or data.

d. If my personal device is lost or stolen, I must report it immediately to the Atlas IT Service Desk.

e. When a personal device is lost/stolen, when an Employee leaves the Company or when there is reason to believe Company data or networks are at risk, a wipe and erase command may be issued. While the Company will take reasonable precautions to only wipe Company data and information (and to prevent personal data from being lost), an automatic wipe and erase command issued by the Company may inadvertently also affect private information and/or the configuration of the device.

f. I will not allow others to use my personal device to access Company information.

g. I will not utilize personal devices that are "rooted" or "jailbroken" to access Company information.

h. Employees are expected to secure all personal devices whether they are in use and/or being carried.

i. Sensitive data (e.g., client/customer data) and passwords must not be stored on personal devices.

j. The Information Technology ("IT") department reserves the right to refuse, by physical and non-physical means, the ability to connect personal devices to corporate and corporate-connected infrastructure, including Employee WIFI internet connectivity.

5. ***Other User Rules***. To ensure the use of the System efficiently and consistent with this Code of Conduct, I may or shall:

a. Use the System primarily for authorized business activities.
b. Use Internet/intranet relay chat channels to conduct official Company business, including obtaining technical or analytical advice.
c. Access databases that I am authorized to access for information as needed for business purposes and use my work e-mail primarily for business contacts.
d. Observe all copyright and license agreements.
e. Exercise computer and network etiquette, including being polite and professional, and using appropriate language, in communications.
f. Use best efforts to protect the privacy of other individuals and abide by all Company, contractual, and legal requirements related to privacy and data protection. This includes not revealing their residence addresses, phone numbers, or other personally identifying information without their prior explicit written permission. I understand that providing my own information is a personal choice.
g. Use best efforts to validate the authorship and/or authenticity of all e-mail messages, attachments, and links received while using the System and to prevent phishing attacks, ransomware, privacy breaches, and other social engineering attempts. Report to the Atlas IT Service Desk when unsure.
h. Comply with applicable Company requirements regarding the retention of Company data.

I shall not:

a. Disrupt the operation of the Company network or the networks of other users or use the System in such a way that it disrupts its use by others. (Significant network traffic can be generated and scarce computer resources can be consumed by Internet/intranet use -- do not send files needlessly, send or forward chain letters, “spam” users via widespread distribution of unsolicited mail, etc.)
b. Download any software from the Internet/intranet on my work computer or equipment, with the understanding that all such software downloads will be done through the IT department. The foregoing does not apply to software downloads on my personal device.
c. Allow my use of the System, Employee WIFI, my personal device, and the Internet/intranet, to interfere with my productivity.
d. Copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner.
e. Use my devices (whether corporate or personal) in a manner that is unlawful or unsafe while in the course or scope of my employment or at any other time I am using the System, including but not limited to: unlawfully operating my mobile device while driving or while operating machinery; utilizing illegal or unlicensed software; and/or violating the terms of service of any personally licensed software for the purpose of performing work. I understand that unlawful and/or unsafe use of my mobile device for business purposes is strictly prohibited.
f. Backup Company data utilizing personal cloud-based services.

6. ***Company Rights***. All Messages, files, and information related to the Company or its business, whether created, sent, received, or stored on or through the System, are the property of the Company and should be considered public information. The Company reserves the right, whether or not it exercises such right, to access and monitor all Messages, files, and information on the System and to disclose such Messages, files, and information to persons within or outside of the Company, including to third parties, law enforcement and government officials in response to a subpoena or other valid legal processes. The Company may monitor and record the Internet/intranet sites accessed, and other services used by me, and this information will be available for enforcement of this Code of Conduct and any other purpose. I acknowledge that:

   a. I DO NOT and CANNOT have any expectation of privacy with respect to my use of the System, or any Message, file, or information on the System.
   b. I have been assigned a User ID and have passwords to limit the access of others to the System, but this does not restrict the Company from accessing any Message, file, or information on the System.
   c. E-mail, text, chat, and Internet/intranet transmissions sent to or received from persons outside the Company utilizing the System are not guaranteed to be private.

7. ***Entity Authorizations***. The Company may authorize limited access to the System by another entity (an "Entity User") and may elect to assign a single User ID to an Entity User, which will then have a single password to access the System. The Entity User will be provided a copy of this Code of Conduct prior to obtaining access to the System and is responsible for ensuring compliance with this policy by all individuals accessing the System using the User ID assigned to the Entity User, provided that the use and sharing of a common Entity User ID and password will not violate this policy. The Entity User is also responsible for ensuring that its User ID and password will only be made available to individuals within its organization who are authorized by it and have a need to access the information available to the Entity User through the System and for changing its password to limit such access whenever any individual with access to the User ID and password is no longer authorized to have such access. The Entity User will be responsible to the Company for any damages resulting from a breach of these provisions. Use of the System by the Entity User is an acknowledgment of acceptance of these terms.

8. ***Violations***. Violations of this policy may result in disciplinary action up to and including termination and/or, with respect to non-employee users, termination of access to the System. In addition, the Company may advise appropriate legal authorities of any illegal actions.