



Information Technology Acceptable Use Policy

Document Information

Version Number	1.0
Last Update	15/10/2022
Author	Matthew Coutts
File Name	Cyber Security Policy and Procedure
Document Title	Cyber Security Policy and Procedure
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	20/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	20/10/2022	20/10/2022	Matthew Coutts

1. Purpose

TEG provides computing resources to staff, clients, and affiliates administrative use in support of the company's objectives. TEG strives to provide a robust, resilient, and reliable information technology infrastructure to enable excellence through the effective and innovative use of computers and information technology. Because computing and network resources are shared and limited, individuals should use the systems responsibly in pursuit of administrative functions, and in doing so, are not to infringe on the rights, integrity or privacy of others or their data. In using the computing systems and network, individuals and groups must abide by standards of lawful and ethical behaviour.

2. Agreement

By using TEG's computing, networking and communications infrastructure, each person agrees that information they post on or distribute through the systems or network contains: no obscene or indecent material; no advertising material or promotional material for products or services; no material which constitutes libel, slander or invasion of privacy or publicity rights; no violation of copyrights or trademarks; no incitement to riot or violence; no violation of Company policies and regulations; and no violation of federal, state or local law.

Each person also consents to the following:

Respect for system security.

It is your responsibility to protect the integrity and security of the data in your account and observe all network security practices as required by the Company. You, and you alone, accept responsibility for all matters pertaining to the proper use of your account; this includes choosing safe passwords and ensuring that file protections are set correctly.

You agree not to give away your userid and password, for any reason, or under any circumstance.

You agree not to use someone else's account, either with or without permission.

Secure use of email.

Users are responsible for ensuring that their email account is not compromised due to actioning/responding to emails of a suspicious or dubious nature (e.g., Spam and Phishing emails).

You agree to validate that any attachments received are from a valid and expected source, and that any links in emails are checked/validated prior to clicking them.

You agree to not provide your user account information and/or password to any request for such information by email.

Responsible use of computing and networking.

You agree not to obstruct any others' work by using unnecessarily large amounts of network resources (such as bandwidth and storage space) or deliberately act in a manner that will cause harm to the network.

You agree not to send spam, chain letters, or other mass unsolicited mailings.

You agree not to advertise or conduct non-Company business using company resources.

Respect for copyright.

Unauthorized distribution of copyrighted material is a violation of federal law. In accordance with the Digital Millennium Copyright Act, the Company, once notified of alleged copyright violations, will disconnect from the network the server or computer of the individual(s) involved. The individual who is distributing the copyrighted materials is responsible for any copyright infringement.

Respectful Communication.

You agree to communicate only in ways that are kind and respectful. You agree to not intentionally access, transmit, copy, or create material that violates applicable laws or the Company's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).

Respect for TEG's computing systems and network administration.

You agree to use the systems and network in a way which promotes TEG's mission. Accordingly, you acknowledge and consent that, when it is necessary to perform systems administration, or, to protect TEG's legal interests, network administrators may access your files and data on the TEG computing systems and network. In addition, you consent to monitoring and review of your user id, user activity, files and data on the TEG systems and network, as well as TEG's right to "freeze" or remove access to any files or data which TEG reasonably believes violates User Obligations.

3. Specific Prohibited Actions

You are given access to TEG Company's computing systems and network because they are tools to help you meet your administrative goals. This access, however, is a privilege, not a right. The Company reserves the right to withdraw all privileges in the event of a violation of this policy. Specific prohibited activities and behaviours are defined in but are not limited to the Guidelines for Acceptable Use document.

4. Penalty for Violation

Staff members who violate this policy will be subject to Company disciplinary action. TEG reserves the right to withhold computing privileges from those who do not abide by the letter or intent of this policy document. In addition, any person who violates this policy or

the guidelines for interpreting this policy may also be subject to sanctions up to and including termination.

5. Approval for Exceptions

In the very rare instances where this policy interferes with the fulfillment of a staff members role and/or function, staff may request a written waiver from the Global Head of Enterprise Technology.

6. Additional Information

For further information about this and other information security policies and applicable computing laws and regulations please contact the Enterprise Technology team.