

## Acceptable Use Policy

*version 5*

The purpose of this policy is to outline the acceptable use of computer equipment at **CLIENT**. These rules are in place to protect the employee and **CLIENT**. Inappropriate use exposes and increases risks including virus attacks, compromise of network systems and services, and legal issues.

### Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct **CLIENT** business or interact with internal networks and business systems, whether owned or leased by **CLIENT**, the employee, or a third party.

This policy applies to employees, contractors, consultants, temporary, and other workers and its subsidiaries including all personnel affiliated with third parties and requires the **USER** to be responsible for exercising good judgement regarding the appropriate use of information, devices and corporate resources.

### Policy

- You must ensure through legal or technical means that proprietary information is protected
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of company assets or proprietary information
- You may access, use or share company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties
- Employees are responsible for exercising good judgment regarding personal use
- For security and network maintenance purposes, authorized individuals may monitor equipment, systems and network traffic at any time

## Unacceptable Use

The following activities are strictly prohibited, with no exceptions:

1. In no circumstance an employee authorized to engage in any activity that is illegal
2. Take action that violates of the rights of any person or company
3. Infringe on or allow copyright, trade secret, patent, or other intellectual property theft
4. Accessing company information that is not within the scope of one's work
5. Accessing data, server, or an account for any purpose other than conducting company business
6. Unauthorized copying of copyrighted material of any type
7. The installation of copyrighted software for which the company does not have an active license
8. Exporting software, technical information, encryption software or technology
9. Introduction of malicious programs into the network or server
10. Revealing your account password to others or allowing use of your account by others
11. Making fraudulent offers of products, or services originating from any company account
12. Making statements about warranty, expressly or implied outside of normal job duties
13. Effecting security breaches or disruptions of network communication
14. Executing any form of network monitoring which will intercept data
15. Circumventing user authentication or security of any host, network or account
16. Introducing honeypots, honeynets, or similar technology on the **CLIENT** network
17. Interfering with or denying service to any user **CLIENT** than the employee's
18. Providing information about, or lists of, **CLIENT** employees to parties outside the organization
19. Sending unsolicited email messages, including the sending of "junk mail" or other advertising
20. Any form of harassment via email, telephone through language, frequency, or size of messages
21. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type
22. Any form of gambling online, using company assets or during business hours or work functions

## Policy Compliance

The HelpDesk team will verify compliance to this policy through various methods, including but not limited to, online investigation, business tool reports, internal and external audits.

Related Policies: Data Classification Policy, Data Protection Standard, Social Media Policy, Minimum Access Policy, Password Policy, Clean Desk Policy, Remote Access Policy (WFH)

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# WaterlooIT

waterlooit.com | 519-208-9880

## Agreement Confirmation

DATE \_\_\_\_\_

USER \_\_\_\_\_

SIGNATURE \_\_\_\_\_

*You have read and as appropriate sought clarification or advice and agree to the terms herein.*

USER  
SIGNATURE \_\_\_\_\_

On behalf  
CLIENT \_\_\_\_\_

*Manager, Director or Owner*

SIGNATURE \_\_\_\_\_

### CLIENT NAME

address

city

phone

url