



Acceptable Use of Technology Policy

Purpose:

Acres Enterprises Ltd. equips its employees with a variety of technological tools (including, but not limited to, computers, laptops, tablets, smartphones) to enhance work efficiency. This document sets forth guidelines for the responsible and ethical use of these technologies.

Scope:

This policy applies to all Acres employees utilizing company-provided electronic devices or accessing company systems (including email and internet) for work-related purposes. Employees must recognize that all data stored or transmitted on Acres's technology systems are company property. Acres retains the right to access, replicate, and utilize such information as deemed necessary.

Policy:

Cell Phone Use:

Use of cell phones while driving is strictly forbidden for safety and legal compliance. If job responsibilities require cell phone availability while driving, employees must use hands-free devices or stop the vehicle safely before taking work-related calls.

Electronic Property Management:

1. Employees must safeguard Acres's electronic assets, ensuring their security and upkeep. In instances of loss or damage, employees might bear responsibility for replacement costs. Prompt reporting to the IT Department is mandatory.
2. Acres systems contain confidential information therefore all Acres devices must be protected through robust passwords and passcodes. Alpha-numeric passwords must be at least 12 characters long and include one uppercase letter, one lowercase letter, one number, and one special character. PIN codes must be at least 6 digits long, and both passwords and PIN codes must not be written down or stored in easily accessible locations.
3. Acres actively monitors and records all internet and email activities on its network and reserves the right to inspect any files for policy adherence.

Email and Internet Usage:

1. Employees have no expectation of privacy regarding any information or messages stored or processed using Acres's technology resources, including but not limited to, computers, text, email, internet, and voicemail.
2. Allocation of passwords or access codes does not establish any privacy rights for employees.

Access Control:

1. Access devices are individually assigned and must remain confidential, shared only with the IT Department when necessary.
2. Employees must protect confidential and proprietary information accessible via technical devices to avert unauthorized access or distribution.

Prohibited Activities:

1. Using Acres's network and technology for accessing offensive material, engaging in threats, violence, illegal activities, gambling, or non-business-related solicitations is strictly prohibited.
2. Engaging in illegal activities using Acres resources may result in immediate termination.
3. Intentional distribution of viruses, worms, Trojan horses, or other harmful software through Acres's network is forbidden.
4. Internet facilities may be used for personal purposes during breaks or outside working hours, adhering to this policy.
5. Unauthorized downloading of entertainment content or software is prohibited. All software installations or changes must be formally requested through the IT Department.
6. Misuse of technology for harassment, infringement on third-party rights, or any unauthorized activities is not permitted.

Cyber Security Training and Policy Compliance:

1. Mandatory monthly cyber security training completion is required for all employees.
2. Annual policy acknowledgment and compliance sign-off are compulsory.

Consequences and Non-Compliance:

Non-adherence to this policy may lead to disciplinary actions, including termination, as per the Progressive Discipline Policy.

Agreement and Acknowledgement

All employees of Acres Enterprises, as a condition of receiving the loan and use of any company electronic devices, and/or access to company systems, email, or internet, are required to annually sign a copy of the Acceptable Use of Technology Policy and Agreement.

To maintain continued access to company technology resources, all employees must complete assigned security training annually. This training is designed to ensure awareness and understanding of best practices in technology usage and cybersecurity, aligning with the firm's commitment to maintaining a secure and efficient technological environment.

The original signed copy of the Acceptable Use of Technology Policy and Agreement will be stored by the Human Resources department.

By signing this agreement, I acknowledge that I have read, understood, and agree to adhere to the provisions outlined in the Acceptable Use of Technology Policy and Agreement. I also commit to completing the requisite security training annually to ensure my awareness and compliance with the evolving standards of technology use and cybersecurity within Acres Enterprises.

I am in receipt of:

- ☐ iPhone
- ☐ iPad
- ☐ Laptop
- ☐ Desktop
- ☐ Other

Condition of device(s):

New / Used - If used, please detail any damage

Employee Name: _____

Employee Signature: _____

Date: _____