

Bonfire Acceptable Use Policy

Bonfire Interactive Ltd. | Confidential

Table of Contents

Introduction.....3

General Use and Ownership3

Overview3

Purpose4

Scope4

Policy4

General Use and Ownership 4

Security..... 5

Unacceptable Use..... 5

 System and Network Activities 5

 Email and Communication Activities 6

Policy Exceptions7

Policy Violations7

Introduction

Our customers trust us, and they expect us to protect the data and resources they've shared with us. Part of how we'll uphold that trust is through pre-established policies so we don't need to make key decisions in critical moments. Below, we explain the sections of our acceptable use policy: what each protects against, why a customer may care, and why we think each is important. We don't mean for the Acceptable Use Policy to intimidate, but we do aim for it to be clear.

General Use and Ownership

This section explains policy around separating work activities from personal activities as much as possible. Understand that the systems you use for work, including a company-provided laptop, have a much lower expectation of privacy than systems you own. You may use your company devices for reasonable personal use, but those devices are not yours because:

- If the company is sued, all its devices are subject to discovery, which means opposing counsel will have access to your data.
- When we troubleshoot our systems, company administrators may have access to your data.
- We may terminate an employee, which may include giving another employee access to the terminated employees' devices and accounts.
- If we are breached, outside investigators will likely inspect all use of an account and/or device, no matter its purpose.

Please limit personal use of company-provided devices as much as possible and remember that corporate devices are not your personal property. Our policies are strict so that we do not have to make judgment calls on a case-by-case basis in high-stress situations.

Overview

Bonfire's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Bonfire's established culture of openness, trust and integrity. Instead, the team is committed to protecting Bonfire's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, cloud-based services, electronic mail, web browsing, and FTP, are the property of Bonfire. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is an organizational effort involving the participation and support of every employee and affiliate who deals with Bonfire information, systems and services. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Bonfire. These rules are in place to protect the employee and Bonfire. Inappropriate use exposes Bonfire to risks including malware, compromise of systems and services, data breaches and legal issues.

Scope

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

This policy applies to employees, contractors, consultants, co-ops, and other workers at Bonfire.

This policy applies to all equipment that is owned or leased by Bonfire.

Policy

All employees, contractors, consultants, temporary, and other workers are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, and local laws and regulations.

General Use and Ownership

- Proprietary information stored on electronic and computing devices whether owned or leased by Bonfire, the employee or a third party, remains the sole property of Bonfire. You must ensure that information is protected in accordance with the Data Protection Policy.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.
- You may access, use or share 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 the reasonableness of personal use. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their manager.

- For security and system/network maintenance purposes, authorized individuals within Bonfire may monitor equipment, systems and network traffic at any time.
- Bonfire reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security

- All mobile and computing devices that connect to the internal network or access Bonfire information must comply with the Asset Management Policy.
- Employees must use extreme caution when opening e-mail attachments or clicking on links received from unknown senders, which may contain malware.
- Providing access to another individual, either deliberately or through failure to secure access, is prohibited.
- Employees must use multi-factor authentication to authenticate to corporate accounts whenever available.
- Employees must use a password manager to avoid insecure, reused or shared passwords with accounts.
- Employees must encrypt their devices if asked and must not interfere or otherwise reduce the level of encryption or security on their devices.
- Employees must install OS and application updates onto their devices if asked or prompted. Employees should also be proactive about applying OS and application updates to their devices.
- Employees must use antivirus/anti-malware or other approved security software to protect the integrity and confidentiality of their laptops if asked and must not interfere or otherwise prohibit security software/configuration on their devices.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing Bonfire-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are prohibited

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not

limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by the company.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted media and the installation of any copyrighted software for which the end user does not have an active license is strictly prohibited.
- Introduction of malicious programs into the network, servers or services (e.g. malware, viruses, worms, trojan horses, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server, service or account that the employee is not expressly authorized to access, unless these duties are within the scope of their role.
- Port scanning or security scanning is expressly prohibited unless the Security team is notified in advance.
- Executing any form of network monitoring which will intercept data not intended for the employee’s host unless this activity is a part of the employee’s normal job/duty.
- Circumventing or bypassing security controls of any host, network, service or account.
- Interfering with or denying service to any user other than the employee’s host (for example, distributed denial of service (DDoS) attack).
- Providing information about, or lists of, employees to parties outside Bonfire.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company.

- Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Creating or forwarding “phishing”, “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of newsgroups or mailing lists (newsgroup spam).

- Use of unsolicited email originating from within Bonfire networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via Bonfire's network.

Policy Exceptions

Any exception to the policy must be approved by Bonfire in advance, and if applicable, documented in the Bonfire Risk Register.

Policy Violations

In the event that a violation of this policy occurs, Bonfire will employ disciplinary measures that reflect the severity of the offence up to and including termination of employment.

Some violations may indelibly affect Bonfire's business in a negative fashion. In this case, punitive measures, including legal action may be pursued.