

Bonfire Information Security Policy

Bonfire Interactive Ltd. | Confidential

Table of Contents

Introduction.....	4
Security Team	4
Security Training	4
Security Awareness Training	4
Secure Coding Training	4
Acceptable Use Policy	4
Access Control	5
Access Requests	5
Account Audits	5
Revocation: Role Changes & Termination	5
Passwords and Accounts	5
Account Sharing.....	5
Password Generation	6
Managing and Storing Passwords.....	6
Password Reuse	7
Multi-Factor Authentication	7
Email Security & Phishing	7
Data Not Suitable for Email Communication	7
Authentication Data.....	7
Confidential Client Data	8
Personal Email	8
Appropriate Email Use.....	8
Sharing/Forwarding Email	8
Phishing.....	8
Computer and Device Security	9
Bring Your Own Device (BYOD) Policy.....	9
Computer Locking	9
Removable devices	9
Untrusted Networks	9
Personal Use of Bonfire systems	10
Software Updates	10
Incident Management	10
How to Report a Security Incident	10
Physical Security	10
Physical Office Access.....	11
Security Surveillance	11
Fire Alarms & Emergency Exits	11

Visitor and Guest Access 11

 Visitor Sign-In..... 11

 Guest Access to Bonfire Systems..... 11

 Guest Wireless Use 12

Unauthorized Visitors 12

Contractors and Service Vendors..... 12

Deliveries 12

Policy Exceptions 12

Policy Violations 12

Introduction

Bonfire has been trusted with \$10's of billions purchasing decisions to date by a range of public and private organizations in Canada, the USA, and internationally. Our top priority has been ensuring a safe, private, and performant cloud / SaaS product. This priority remains unchanged while we expand our client base and product functionality now and in the future.

We recognize the sensitive and mission-critical nature inherent in our clients' use of Bonfire and have implemented specific policies and practices that govern our infrastructure and activities.

Security Team

The Bonfire Security Officer is accountable for creating and enforcing security policies and procedures; monitoring, vulnerability management, and incident detection and response initiatives; and tracking and reducing risk organization-wide.

The Bonfire security team is responsible for carrying out all security policies and procedures. The team is made up of resources from different parts of the business as necessary.

Security Training

Security Awareness Training

Bonfire employees and contractors are provided training on the company's security policies and procedures during their first 30 days of employment and annually thereafter. All Bonfire personnel are then required to acknowledge that they have the attended training and understand the security policies of the company.

Secure Coding Training

Bonfire employees and contractors in developer roles are provided with SDLC / Secure Coding training during their first 30 days of employment and annually thereafter. Software developers are trained in secure coding techniques, including how to avoid common coding vulnerabilities. All such personnel are then required to acknowledge that they have attended and understand secure software development lifecycle (SDLC) training and OWASP Top Ten common coding vulnerabilities.

Acceptable Use Policy

Bonfire's Acceptable Use Policy covers employee responsibilities and behavior for using Bonfire systems, including devices, email, internal tools, and social media. Bonfire employees must acknowledge that they have read and will abide by the Acceptable Use Policy. All of Bonfire's security policies, including the Acceptable Use Policy, are presented to new

employees during onboarding, and all employees are required to sign off that they have read all such policies.

Access Control

Access to Bonfire systems, customer data and third-party accounts owned by Bonfire will only be granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of that position. Access is always provisioned following the principle of least-privilege.

Access Requests

Access requests for Bonfire employees are made by employees and their managers. Requests are to be made to the IT team for managed IT services or the owner of the service for which access is being requested.

Employees will not be granted access unless it is deemed that the access is necessary to complete a necessary business task.

All access grants are scoped to the minimum breadth and duration to complete the relevant business task. Root access will not be granted unless absolutely necessary to perform the job function.

Account Audits

The IT, Security and DevOps teams will conduct quarterly audits of accounts, privileges and password management, and are required to document findings and remediation plans.

Revocation: Role Changes & Termination

- Managers must notify Bonfire's IT team if an employee has been terminated or changes roles.
- In the case of termination, the former employee's access is required to be revoked within reasonable timelines.
- In the case of a role change, the employee's access should be reviewed and revised within reasonable timelines.
- In some cases, access may be revoked due to a policy violation or incident.

Passwords and Accounts

Account Sharing

By avoiding the sharing of accounts, we achieve a higher level of security and decrease the amount of data that could be exposed when a single account is compromised.

Bonfire employees are not to share passwords with anyone. Create your own account rather than using a shared account whenever possible.

Password Generation

Bonfire employees must use passphrases or complex passwords, where possible, for all of their accounts that have access to Bonfire data.

Complex passwords have a combination of uppercase letters, lowercase letters, numbers, non-alphanumeric “special” characters.

A **passphrase** is a series of words or a sentence that you can remember but would be difficult for someone else to figure out

The below are requirements for passwords:

- User account passwords should be at least 14 characters in length.
- System or service account passwords should be at least 24 characters in length.
- Use of long passphrases are strongly urged to be used for passwords that need to be remembered.

Managing and Storing Passwords

Using unique, long, and complex passwords can make it difficult to remember all of your passwords. It can also be difficult to come up with many unique passwords.

To help solve this problem, Bonfire uses a password management tool called 1Password to help you manage your passwords and overcome these difficulties. 1Password will help you to create passwords, store them, and autofill login forms.

Once you have 1Password set up you only need to remember the 1Password master password and your laptop password. All other passwords will be stored in the password manager, so you won't have to remember them.

Employees are required to use 1Password to manage their passwords and generate sufficiently complex passwords. Use 1Password and secure it with a strong password or long passphrase (minimum 14 characters).

All Bonfire system and user passwords must be encrypted when stored at rest within an application or database. At no time should passwords be written down on post-it notes or whiteboards. All Bonfire system and user passwords must be encrypted during transmission and only sent over secure channels. Under no circumstances should Bonfire employees share their account passwords with anyone, including other Bonfire employees.

Password Reuse

The same password should not be used for two or more accounts. When a password is reused, a security breach on one site can compromise the security of your account on another site. For example, in 2012 LinkedIn was hacked and over 6 million passwords were stolen. Many people used the same password for LinkedIn as for other sites. Hackers were then able to try this list of passwords against other sites.

- All generated passwords for Bonfire users and system accounts must be unique and never used across multiple systems, sites or services.
- Bonfire employees may not reuse passwords that are or were used elsewhere, e.g. passwords used for personal accounts.

Multi-Factor Authentication

Multi-factor authentication (MFA), also known as two-factor authentication, is an authentication system that involves having both a login/password and a physical device that provides a code. When you log in with such a system you will typically need to log in with your username and password, then provide the current code from your physical device. The physical device can be a dedicated dongle, or a phone using an MFA app such as Google Authenticator, Authy, and 1Password.

MFA is more secure than just username and password alone, because if your password is stolen an attacker can still not log in without the physical device.

Email Security & Phishing

Email is a ubiquitous and valuable communication tool, but care must be taken to ensure that is used in an appropriate and secure manner. Bonfire strives to ensure that email is used in a way that protects client data.

Data Not Suitable for Email Communication

Not all data is suitable to be included in emails. Care must be taken to avoid sending any such data. Such data types are explained below, including circumstances under which they may or may not be included in email.

Authentication Data

Authentication data is not to be sent via email under any circumstances. Authentication data includes; passwords, SSH keys, API keys, security question responses or any other information that may be used to authenticate against internal or external systems.

Confidential Client Data

Confidential client data may not be included in email communication with third parties without the permission of the client. When communicating with employees of the client company, information may only be disclosed via email that the employee has access to via their bonfire credentials, or that is appropriate to their position, unless permission is granted by the client.

Personal Email

Bonfire employees shall not use Bonfire email accounts to send or receive personal emails.

Bonfire employees shall not use personal email accounts to send email on behalf of Bonfire or relating to Bonfire business.

Appropriate Email Use

Bonfire employees will only send emails relating to their role / function. Clients are not to be contacted via email unless appropriate to the employee's role.

Sharing/Forwarding Email

Care should be taken to share or forward emails only as necessary. The same rules that apply to sending email apply to forwarding with regard to client permission and appropriate use.

Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card numbers, often for malicious reasons, by masquerading as a trustworthy entity. Phishing is one of the most common and effective ways that a company can be attacked. Here are some of the forms that phishing can take:

- Embedding a link in an email that redirects you to an unsecure website that requests sensitive information.
- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information.
- Spoofing the sender address in an email to appear as a reputable source and requesting sensitive information.
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.
- Convince the employee to visit a malicious site in an attempt to infect their browser/computer, steal account credentials or steal company/customer data.

Phishing attacks can often be prevented by being suspicious of emails or requests for information that come from untrusted sources, or that are unusual.

Computer and Device Security

Bring Your Own Device (BYOD) Policy

Bonfire provides employees with devices that conform to our policies. However, Bonfire employees may, from time to time, access company information using their own devices, including mobile devices. All employee-owned devices **must** conform to Bonfire security policies and standards if they're used to access Bonfire data, systems, and/or IT infrastructure.

Computer Locking

One of the simplest ways that Bonfire's security could be compromised would be for an attacker to walk into our office and take an unattended laptop. If such a laptop were left unlocked, the attacker would gain immediate access to Bonfire data. In addition to supervising all visitors to the office, locking laptops prior to leaving them unattended provides us with additional security. Your laptop should never be unattended and unlocked.

Removable devices

Media (e.g. USB drives, external hard drives, CD-ROMs) from unknown or untrusted sources are not to be connected to Bonfire computers. Such devices may contain malicious programs which could compromise security.

There is also a chance that Bonfire company or customer information may be saved to a removable device which may not have adequate protections, e.g. encryption.

Bonfire employees are not to connect untrusted devices such as USB keys or storage devices to your computer. Should a valid business request require storage of Bonfire or customer data on removable media then the request needs to be approved and sufficient controls be applied (e.g. encryption).

Untrusted Networks

It is possible for a network to intercept all communication between your device and the internet, and this is becoming an increasingly common tactic used by malicious parties to gain sensitive data. Even when using ssl on untrusted networks you are vulnerable to various attacks. For this reason, you should avoid connecting any devices that hold Bonfire data (e.g. your laptop and phone) to untrusted networks. Your home WiFi, or the office WiFi can be considered trusted but public networks, particularly those with no password, are not trusted.

Bonfire's network (WiFi and Ethernet) should be considered as an employee-only resource. Keeping non-employees off the Bonfire network provides us with an additional level of protection.

If you have guests in the office that require internet access, please have them connect to the Bonfire-Guest network.

Personal Use of Bonfire systems

Bonfire allows personal use of laptops but please be aware of the sites and services that you use. Websites with pornographic content and torrenting sites often contain malware, please avoid visiting such sites on your Bonfire laptop.

You should also be careful with the installation of software and browser extensions. Extensions often request a large range of privileges and, if granted, can track most of what you are doing online, circumvent security controls and even steal your information.

Software Updates

Apple regularly releases software updates for your Mac. Chrome, Safari and Firefox regularly release updates to their browsers. Please ensure that you install these updates in a timely manner, along with updates to other tools that you may be using. Often these updates include security related fixes that are required to keep you protected from the latest attacks.

Bonfire employees are expected to apply updates to your computer and browser as they become available and not delay beyond a reasonable amount of time.

Incident Management

Bonfire's Support and Incident Management Policy describes how bonfire determines and responds to incidents. All Bonfire employees have a responsibility to report incidents in a timely manner.

How to Report a Security Incident

Below are ways to report a **security incident**

- Email security@gobonfire.com
- Message #general, #it, or #security on Slack.
- Create a service desk IT ticket - <https://bonfirehub.atlassian.net/servicedesk/customer/portals>
- Contact your manager

It is important to include as many specifics and details as you can.

Physical Security

Bonfire's Physical Security Policy describes how staff should permit access to and secure the Bonfire office.

Physical Office Access

Physical access to Bonfire's office is restricted using access cards for which only Bonfire employees, approved contractors and building management have keys.

- Bonfire's office remains locked throughout the entire day.
- Bonfire's office is an open space concept for collaborative reasons.
- Bonfire reviews key and access card access as deemed necessary to ensure keys and cards are accounted for.
- If access cards are lost or stolen, they are to be disabled in the business access system and building management is notified.
- All physical and logical access is revoked upon termination of Bonfire employees or contractors.

Security Surveillance

The building in which Bonfire leases office space has security cameras at entrances and key locations.

Fire Alarms & Emergency Exits

Fire detectors and emergency exits are installed and located according to applicable laws and regulations.

Visitor and Guest Access

Bonfire employees may invite visitors to the office for business reasons or during pre-specified times, for social reasons. Bonfire staff must escort and supervise their visitors at all times and are responsible for the visitor's behaviour while they are in the office.

Visitor Sign-In

All visitors are required to sign in at the visitor kiosk located at the main entrance. The Envoy visitor management system is used to register new visitors, digitally record NDA agreements and notify hosts of a visitor's arrival.

Bonfire does not have a public lobby but does have a waiting area outside of the office where visitors can be greeted by their hosts and escorted into the office.

Guest Access to Bonfire Systems

Occasionally, guests will have a legitimate business need for access to the corporate network. When such need is demonstrated, temporary guest access to company systems is permitted. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

Guest Wireless Use

Bonfire's production systems are not accessible directly over wireless channels and connecting to the company guest wireless network should grant no extra privileges or access to company systems.

Unauthorized Visitors

It is the responsibility of all Bonfire employees who spot an unauthorized visitor to either ask the unauthorized person to leave or to notify their manager.

Contractors and Service Vendors

Contractors, suppliers and service vendors, e.g. IT technicians, cleaning staff, coffee service personnel, may enter Bonfire's office to complete their job duties.

Deliveries

Anyone who delivers orders, mail, or packages for employees are to follow instructions located at the office entrance or ring the doorbell for assistance.

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 Bonfire policies occur, 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.