

Bonfire Operational Controls Policy

Bonfire Interactive Ltd. | Confidential

Table of Contents

Introduction	4
Risk Management Program	4
Definition of Risk.....	4
Risk Principles	4
Risk Analysis at Bonfire.....	5
Scope.....	5
Components of Risk Management.....	5
Threat.....	5
Likelihood	5
Consequence	6
Risk Assessment	6
Risk Management	6
Risk Owner.....	6
Risk Assessment & Management Policy.....	6
Risk Assessment Process.....	7
Risk Mitigation and Acceptance Standards.....	8
Responsibilities for Risk Management.....	9
Vendor Management Policy	9
Vendor Risk Assessments	9
Vendor Assessment Process	10
Vendor Assessment Due Diligence	11
Vendor Compliance Considerations	11
Managing Vendors	11
Vendor Supervision	11
Vendor List.....	11
Data Center Supplier Requirements	12
Minimum Requirements	12
Additional Requirements	13
Data Redundancy and Fault Tolerance	14
Load Balancing	14
Database.....	14
Database Fail-Over	14
Database Replication	14
Database Backups	14
Document Storage.....	14
Malware Protection	14
Network	15
Availability Zones.....	15
Subnets.....	15
Public Subnet.....	15
Private Subnet	15
Security Groups.....	15

Change Management – Code Deployment 15

Version Control	15
Branching Model.....	16
Production branch.....	16
Staging branch.....	16
Development branch.....	16
Feature branches.....	16
Security bugs.....	16
Hotfix branches.....	17
Change Initiation	17
Pull Requests.....	17
Code Reviews, Change Review, and Change Approval.....	18
Merging a Pull Request.....	18
Deployment.....	18
Zero Downtime Deployment.....	19

Vulnerability & Patch Management 19

Vulnerability Management & Patch Policy	19
Vulnerability Scanning.....	19
Penetration Testing	19
Bug Bounty Program	19
Patch Severity & Timing	20
Low Severity - 0.1 - 3.9.....	20
Medium Severity - 4.0 - 6.9	20
High Severity - 7.0 - 8.9.....	20
Critical Severity - 9.0 - 10.0	20
Patch Installation.....	20

Asset Management Policy 20

Asset Standards	21
Configuration Standards.....	21
Variations to the Configuration Standard	21
Bring Your Own Device (BYOD) Policy.....	21
Software Licensing Guidelines	21
Technical Support and Maintenance Practices.....	22
Configuration Management Guidelines.....	22
Asset Inventory Practices	22
Asset Disposal Guidelines.....	22

Policy Exceptions 22

Policy Violations 23

Introduction

Internal operational controls are essential to maintain system confidentiality, integrity and availability. Bonfire strives to ensure commercially reasonable methods to configure our service offering to maintain SLA uptime requirements, and security objectives.

Risk Management Program

In an environment of significant change, it is essential that Bonfire recognizes the importance of assuming a reasonable level of risk if it is to fulfill its vision, mission, and strategic priorities. In order to grow and continue to be a best-in-class product, Bonfire needs to push forward which often involves taking risks. Not all risk can be transferred to third parties through insurance policies, contracts or waivers, as such the management of residual risk at all levels of the organization is imperative.

Bonfire is committed to building increased awareness and a shared responsibility for risk management at all levels of the organization. This policy is intended to assist in decision making processes, support the acceptance of risk, improve the management of existing uncertainty and the approach to new opportunities.

Definition of Risk

Bonfire defines risk as the possibility that an uncertain event, action or set of circumstances which, if to occur, would have a material adverse effect.

Risk Principles

Bonfire is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realized.

Bonfire has the primary duty to ensure the Security, Availability, and Confidentiality of critical systems and customer data. A duty to ensure a secure, available infrastructure requires Bonfire to identify and manage risks.

Bonfire believes that effective risk management involves:

1. A commitment to the Security, Availability, and Confidentiality of Bonfire infrastructure and services from senior management;
2. The involvement, cooperation and insight of all Bonfire staff;
3. A commitment to initiating risk assessments, starting with discovery and identification of risks;
4. A commitment to the thorough analysis of identified risks;
5. A commitment to a strategy for treatment of identified risks;

6. A commitment to communicate all identified risks to the company;
7. A commitment to encourage the reporting of risks and threat vectors from all Bonfire staff.

Bonfire believes that the following events can trigger a risk assessment to occur:

- A significant and major change to existing infrastructure, product or business practices;
- A significant amount of time (e.g. a year) having passed since the last risk assessment.

Risk assessments can be as high level or detailed to a specific organizational or technical change as Bonfire stakeholders and teams see fit. Risk assessments can be conducted by unbiased and qualified parties such as security consultancies or qualified internal staff.

Risk Analysis at Bonfire

Bonfire performs its risk analysis following qualitative risk analysis principals.

Scope

This Risk Management program and policy applies to all systems and data that makes up the Bonfire system, owned by Bonfire or its customers, or operated on behalf of the organization.

Risk assessments should evaluate infrastructure such as computer infrastructure containing networks, instances, databases, systems, storage, and services.

Bonfire risk assessments will also include an analysis of business practices, procedures, and physical office spaces as needed.

Risk assessments for vendors are covered under Bonfire's Vendor Management Program, which includes a risk assessment targeted at a vendor's security and business practices.

Components of Risk Management

Threat

A potential incident or activity which may be deliberate, accidental, or caused by nature which may cause physical harm to a person or financial harm to an organization.

Likelihood

Likelihood is a qualitative description of probability or frequency. The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

Consequence

Consequence is the outcome of an event and is a loss, disadvantage, or gain. There are a range of possible outcomes associated with an event. Consequence and impact are used interchangeably. The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Risk Assessment

A risk assessment is the process of evaluating and comparing a level of risk against predetermined acceptable levels of risk. It is an examination of all possible risks along with implemented and non-implemented solutions to reduce, eliminate, or manage the risks.

Risk Management

Risk management is the application of a management program that addresses organizational and technical risk. This management program includes identification, analysis, treatment, and monitoring.

Risk Owner

A risk owner is the person responsible for managing an individual risk. The risk owner is typically the person directly responsible for the strategy, activity, or function that relates to that risk.

Risk Assessment & Management Policy

This risk assessment policy specifies how and when risk assessments will be done and who will be responsible for conducting risk assessments and implementing solutions to address any findings.

It is the responsibility of all Bonfire staff to identify, analyze, evaluate, monitor, and communicate risks associated with any activity, technology, function, or process within their relevant scope of responsibility and authority. Staff identifying potential risks or vulnerabilities are to report them to Bonfire's Security Team.

Overall, the execution, development, and implementation of risk assessments and remediation programs is the joint responsibility of Bonfire's Security Team and the department or individuals responsible for the surface area being assessed. All staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan for each risk assessment performed.

- Bonfire performs at least one assessment yearly using qualified internal staff or external vendors/contractors who have experience performing risk or technical security assessments.
- A risk assessment should be performed on critical systems and applications no less than every two years.
- Risk assessments may be used to assess all risks to the organization.
- All staff involved with a risk assessment must fully cooperate with the risk assessment project lead in conducting the assessment and developing a remediation strategy.
- Any staff members or external consultants who perform any Bonfire risk assessments are required to be familiar with computer technology and computer security in particular.
- Risk assessment deliverables include an assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks. The action plan may be included with the report, or separately. The action plan will be a plan for implementing additional controls and solutions to mitigate or manage the risk.
- The risk assessment process and methodology used will be updated as required due to scope of the assessment, or results of audits and incidents.
- All identified vulnerabilities will be assessed for impact and criticality. Vulnerabilities must be remediated as soon as possible as set by the Bonfire Vulnerability and Patch Management Program.

Risk Assessment Process

Bonfire risk assessment methodology may be based on [*NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments*](#).

- Bonfire Management defines the scope of risk assessment and creates the risk assessment team with a point person to guide the process.
- If risk assessment procedures are not defined, the team should define them. The proper time and method of communicating the selected risk treatment options to the affected IT and business management should be included.
- Evaluate the system - Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system according to the Bonfire Data Classification Policy, considering Security, Availability and Confidentiality needs.
- List the threats - List possible threat sources such as an exploitation of a vulnerability.
- Identify vulnerabilities.
- Evaluate potential security controls already in place to assess if they adequately address the risk.
- Identify probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.

- Quantify damage (impact) - Categorize the damage and possibly place a dollar amount on the damage where possible. This will help when looking at the cost of controls to reduce the risk.
- Determine risk level - Use likelihood times impact to quantify the amount of risk.
- Evaluate and recommend possible controls to reduce or eliminate risk - Identify existing controls and those that may further reduce probabilities or mitigate specific vulnerabilities. List specific threats and vulnerabilities for the system to help identify mitigating controls.
- Create the assessment report.
- Communicate the selected risk treatment options to the affected IT and business management and staff.
- Take recommended risk mitigation actions.
- Monitor the effectiveness of the risk mitigation actions.

Risk Mitigation and Acceptance Standards

Options for mitigating risk shall include the following possibilities:

- Reducing the chance of an occurrence of an event
- Reducing the damage due to occurrence
- Avoiding the risk
- Transferring the risk by taking an action such as purchasing insurance
- Accept the risk

Some guidelines and standards applicable to Bonfire

- Costs of implementing each control are considered and compared to the benefits of implementing each control.
- Cost and benefit analysis is done to evaluate proposed controls versus risks. When the controls are evaluated, the benefits, costs, and cost savings of applying the controls both individually and in combination should be determined. Performance measures for determining the effectiveness of the new controls are created.
- Risks shall be ranked, and controls are selected, and a plan created to implement the controls. Responsibilities for implementing the controls are determined and communicated. Budgeting and schedules are set and the expected outcomes from mitigating the risks with the controls are documented. Residual risk after full implementation is considered.
- Decisions regarding residual risk are made. Specifically, whether to accept the risk, transfer the risk, or take other action, including adding additional controls.
- Safeguard options (e.g. insurance) for addressing high risk scenarios must be considered and utilized appropriately while the extent of risk reduction and benefits are considered. Cost and benefit analysis is done to evaluate safeguard options.

- If the cost of safeguard options or recommended risk controls is greater than the available budget, the options and controls are prioritized to reduce as much risk as possible within the budget.
- When the risk assessment report is completed, results shall be communicated to the affected IT and business management and staff.

Responsibilities for Risk Management

The Security Team is accountable for the Bonfire risk management program, communicating detected risks and remediation steps needed to the appropriate staff for resolution. Those staff members are then responsible for resolving the detected risks in a timely manner, guided by the severity of the detected risk.

Every staff member at Bonfire is responsible for identification of potential risks and to report them to their leadership.

Managers and Executives are responsible for the development of risk mitigation plans and the implementation of risk reduction strategies. Risk management processes should be integrated with planning processes and management activities.

Vendor Management Policy

Bonfire relies on vendors to perform a range of services, some of which are critical for operations.

Bonfire aims to manage its relationship with vendors and minimize the risk associated with engaging third parties to perform services. This policy provides a framework for managing the lifecycle of vendor relationships.

Vendor Risk Assessments

For each potential vendor, an initial risk analysis, assigning the vendor a “low,” “medium,” or “high” rating is conducted based on the highest risk level attributable to the contract.

	Low	Medium	High
Business impact	Nominal impact, could get along without it. Does not connect to any piece of Bonfire service infrastructure.	Significant but non-critical business impact	Mission critical

Customer facing?	No	Indirect	Direct
Access to customer data	No access	Access to often public but personally identifiable information (e.g. email addresses)	Access to non-public personally identifiable information (e.g. email content)

The rating indicates the level of due diligence Bonfire requires for each vendor:

- **Low-risk** vendors typically require little analysis
- **Medium-risk** vendors should be evaluated to determine the appropriate level of due diligence required
- **High-risk** vendors require extensive review

Vendor Assessment Process

Vendor assessments should be conducted before doing business with a new vendor and revisited when the relationship with the vendor changes significantly, including contract renewals.

An assessment of the proposed vendor is initiated when a Vendor Sponsor (anyone at Bonfire looking to do business with a vendor) submits a request to add a new vendor or renew a vendor contract.

The Vendor Sponsor must sign a mutual Non-Disclosure Agreement (mNDA) with the proposed vendor if internal Bonfire details will be discussed such as:

- discloses Bonfire information to determine company/vendor fit
- purchase contract does not include an implied non-disclosure agreement, but Bonfire internal information will be disclosed to the vendor.

When a mNDA is required, the proposed vendor should sign the mNDA before the Vendor Sponsor.

The Vendor Sponsor should then submit the mNDA (if applicable), and vendor assessment questionnaire (VAQ) responses, and other relevant collateral to the Finance and Security teams for review.

The Finance and Security teams will complete the review and communicate next steps to the Vendor Sponsor. All reviews should be documented and, if applicable, risks entered into the risk register.

Vendor Assessment Due Diligence

Due diligence entails making a reasonable inquiry into a vendor's ability to meet the requirements for the proposed service. Bonfire may send the proposed vendor a Vendor Assessment Questionnaire (VAQ) to gather important information about the service. Once the VAQ is completed, the Security and Finance teams review the responses and either clears the vendor, rejects the vendor, or requests further information.

A due diligence review might include further discussions regarding the following topics:

- **Regulatory:** Can the vendor create regulatory risk for Bonfire?
- **Reputation:** How might the vendor impact Bonfire's reputation?
- **Financial:** Can the vendor impact Bonfire or its customers financially?
- **Access to customer data:** To what extent will the vendor handle sensitive Bonfire data?
- **Operational effectiveness:** How might Bonfire be affected if the vendor experienced downtime? If the vendor ceased operations suddenly? Are there other potential vendors that Bonfire could work with in such cases?
- **Compensating controls:** Does the vendor offer multi-factor authentication on its service? Data encryption? Security monitoring? Other security controls.

Vendor Compliance Considerations

If the vendor has a SOC 2, ISO 27001/2, or other relevant collateral, it should be collected, reviewed by the Security Team, and documented.

Managing Vendors

Vendor Supervision

Each vendor will be assigned a Vendor Sponsor/Owner who will act as a liaison between the vendor and Bonfire.

Vendor List

The Finance and IT teams maintain a complete list of all vendors (freemium and paid) along with the Bonfire employee who is the Vendor Sponsor/Owner assigned for the Vendor/Tool

Data Center Supplier Requirements

Bonfire's minimum requirements for use of third-party data centers in the delivery of its software and services. This serves as (1) an internal guide for Bonfire staff in choosing appropriate data center suppliers, and (2) an assurance to Bonfire's customers and partners that appropriate data center suppliers are utilized in the delivery of its software.

Minimum Requirements

The following requirements are the Minimum Performance Levels (MPLs) acceptable for a datacenter to be approved for use in Bonfire's product delivery:

Connectivity Requirements	MPL
Connectivity – Bandwidth Provider	'Tier 1' bandwidth provider connection (also known as 'transit-free network' connection)
Connectivity – Server Incoming Bandwidth	100 Mbps incoming connection
Connectivity – Server Outgoing Bandwidth	100 Mbps outgoing connection
Connectivity – Availability	99.9% up-time guarantee
Connectivity – Scheduled Maintenance Notice	48 hours notice

Security & Data Integrity Requirements	MPL
Security – Security Monitor	Network-based, OS integrity checks, intrusion detection.
Security – Physical Access to Servers	Restricted to authorized personnel only. Physical security system in place to prevent unauthorized physical access.
Data Integrity – Access By Data Centre Staff	Prohibited except with explicit permission
Data Integrity – Data Access Logs	Log all data center staff access to server
Data Integrity – Information Sharing	Information sharing with third parties is strictly prohibited.

Hardware Requirements	MPL
-----------------------	-----

Hardware – Power Supply	2x redundant power supply to server. Backup power system capable of providing five (5) days uninterrupted power to the server.
Hardware – Parts Replacement	Faulty or defective parts of server replaced within defined service windows or pre-emptively as part of scheduled maintenance.

Support Requirements	MPL
Support – Active Monitoring	24 / 7 monitoring by on-site technicians year- round
Support – Phone & Email Availability	24 / 7 phone support, year-round 24 / 7 email support, year-round
Support – Minimum Response Time (Level 1 Issue*)	1 hour or less
Support – Minimum Response Time (non-Level 1 Issue*)	12 hours or less

* Level 1 in this context refers to total server unavailability or faulty components.

Additional Requirements

In addition to the above, Bonfire’s choice of data center suppliers may also be subject to the following conditions / restrictions:

Additional Requirements	MPL
Location of Data Centre	Data centers must be located in specific countries or region (e.g. Canada, USA, Europe, etc.). This requirement is specified on a Customer’s Order Form.
Server Specifications	Data centers must offer servers with suitable technical specifications for a particular deployment (e.g. RAM, CPU speed, etc.).

Data Redundancy and Fault Tolerance

The purpose of this document is to Bonfire's approach to ensuring the availability and integrity of its systems. This is achieved both through fault tolerance (the ability of the system to continue to operate in the presence of various issues) and redundancy (having duplication of critical components).

Load Balancing

Bonfire application servers run through a load balancer. This means that requests made to the application are sent to a service that distributes the requests between multiple redundant servers. The load balancing service continuously runs health checks against these servers and will stop directing requests to any server that is deemed unhealthy. In the event of server failure, requests are simply routed to the remaining health servers.

The load balancing service itself is robust, automatically scaling and highly fault tolerant.

Database

Database Fail-Over

Bonfire utilizes a relational database service that provides a seamless failover feature. The database exists in two geographically separate locations with one of these instances actively serving application data requests. If the active instance is in a failure state or is unavailable, the service will automatically fail-over to the second instance.

Database Replication

In addition to the fail-over capability, Bonfire maintains a separate read-replica of the database. If data should somehow be corrupted, or if both primary instances are unavailable, the read-replica is available for manual switch over to master status.

Database Backups

Please refer to the Backup Policy for details of how Bonfire ensures additional redundancy via database backups.

Document Storage

Bonfire uses a document storage service that is both redundant and fault tolerant, including geographically distinct storage. Data integrity is regularly checked, and any corrupt data is repaired using redundant data.

Malware Protection

Bonfire uses anti-malware protection to scan applicable supplier documents and data within the Bonfire portal. Virus definitions are updated daily.

Network

Availability Zones

Bonfire distributes all of its services across two independent, geographically isolated availability zones, within the data region (US, EU, CA).

Subnets

Across the availability zones, two sets of subnets exist; one public (accessible to the internet), and one private (accessible within itself).

Public Subnet

The Public subnet serves as the area to allow for inbound traffic to reach our load balancers.

Private Subnet

The private subnet is used for inter-service communication and management functions.

Security Groups

Security Groups are deployed to provide virtual firewall functionality to control traffic between areas of the environment as well as Ingress and egress traffic restrictions.

Change Management – Code Deployment

Bonfire's Change Management Policy describes how changes to the Bonfire system are proposed, reviewed, deployed, and managed. This policy covers all changes made to the Bonfire system, regardless of their size, scope, or potential impact.

This policy is designed to mitigate the risks of:

- corrupted or destroyed information
- degraded or disrupted computer performance
- productivity losses
- introduction of new vulnerabilities, configuration errors and software bugs in infrastructure and code
- exposure to reputation risk

Version Control

All of our software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role.

Using a decentralized version control system allows multiple developers to work simultaneously on features, bug fixes, and new releases; it also allows each developer to work on their own local code branches in a local environment.

All code is written, tested, and saved in a local repository before being synced to the origin repository. Writing code locally decouples the developer from the production version of our code base and insulates us from accidental code changes that could affect our users. In addition, any changes involving the persistence layer (database) are performed locally when developing new code, where errors or bugs can be spotted before the change is deployed to users.

Branching Model

Production branch

The *release/production* branch reflects the current state of the application in production.

Staging branch

The *release/staging* branch reflects the current state of the application in the staging environment.

Development branch

The master branch reflects the development changes delivered most recently for the next release and the state of the application used in the test environment.

Feature branches

Feature branches are used to develop new features for a future release, the specifics of which might not be known when development starts. A given feature branch will exist as long as the feature is in development; the branch will eventually either be merged back into master to add the new feature to an upcoming release with a pull request, or discarded (if the feature will not be added to an upcoming release).

Feature branches are typically branched from master and are merged back into master. Feature branches typically exist both locally in the developers environment and in the origin (bitbucket).

Security bugs

Bonfire recognizes that security bugs represent key issues that should be resolved quickly to maintain the security, confidentiality, privacy, processing integrity, and availability of the service. Bonfire commits to resolving security bugs within reasonable timelines.

Hotfix branches

Hot fix branches are meant for new, unplanned production releases that address the live system being in an undesired state. A hotfix branch is made up of the *release/production* or *release/staging* branch. This allows team members on the master branch to continue their work while someone else prepares the bug fix.

When finished, the bug fix needs to be merged back into the original branch, so it is deployed to production. The merge should be done through a pull request.

Hotfixes that are merged directly into *release/production*, without going through *release/staging*, are exceptions that should be used only when a critical bug in the production system needs to be addressed immediately.

Permission for a hotfix should be obtained from the Engineering leadership and should be noted in the pull request.

Change Initiation

To initiate a change, the developer first creates a feature branch which represents a proposed change to the codebase.

Code changes are grouped into diffs, each of which represents a proposed change to the codebase.

Pull Requests

When a developer finishes a feature branch, they make a pull request to merge those changes into master. This submits the changes for peer review. For all code changes, the reviewer should be different from the author.

Pull requests allow developers to describe the changes they're making; co-workers can review the set of changes in a code review. Pull requests also trigger automated testing and code-quality checks that must be completed and returned successfully before merging is allowed. Testing and approval are logged by the system.

A pull request's details section should be used to note any non-code changes (e.g. environment or database changes) needed before the commits are merged.

Once tests pass and the code is approved, the author can merge the code to the central repository.

Code Reviews, Change Review, and Change Approval

Before the feature branch is merged, a code review should be performed. Code reviews are performed by a second developer (i.e. not the one who wrote the code), who considers questions like:

- Are there any obvious logic errors in the code?
- Are all cases specified in the requirements fully implemented?
- Is there sufficient automated testing for the new code? Do existing automated tests need to be rewritten to account for code changes?
- Does the new code conform to existing style guidelines?
- Are there any egregious security errors as defined by the [OWASP Top 10](#)?
- Does it meet applicable accessibility requirements?

A code review should take place after all code has been written and automated tests have been run and passed, as this ensures the reviewer's time is spent checking what automation misses.

The reviewer should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.

Once the review process finishes, the reviewer should accept or reject the pull request. Only when the pull request is accepted will the change be merged into the release branch.

Merging a Pull Request

Before merging a pull request, the developer should check that all prerequisites have been met, including environment changes or database migrations. Once non-code changes have been implemented, the pull request can be merged.

If the application is deployed through our standard, zero-downtime development process, the developer's job is complete.

If any of these changes necessitate system down-time, the merge should take place within a scheduled and pre-announced window when customers are less likely to be affected.

Deployment

The system is monitored on a continuous basis. Should the site be negatively affected by a change, that code change is rolled back.

Zero Downtime Deployment

Zero-downtime deployments allow us to make changes without waiting for a change window and allow us to return the application to a previous state easily.

Vulnerability & Patch Management

Bonfire's Vulnerability Management policies and procedures describe what systems are in place to monitor for new vulnerabilities, how often vulnerabilities are addressed, and the way in which those vulnerabilities are addressed.

On average, 20-30 new vulnerabilities are released into the wild every day. Bonfire's internal vulnerability monitoring and external vulnerability scanning are in place to keep up with new threats while validating security controls put in place so that Bonfire's security posture is maintained.

Vulnerability Management & Patch Policy

Bonfire performs internal vulnerability scanning and package monitoring on a consistent basis using:

- AWS Inspector
- Vanta
- Apple
- Jamf Pro
- Various security feeds & blogs

Vulnerability Scanning

Bonfire performs external vulnerability scanning weekly against the Bonfire service using tinfoilsecurity.com

Penetration Testing

Full Application and infrastructure penetration testing is conducted on an annual cadence to identify gaps and exposures that could be leveraged by an attacker.

Bug Bounty Program

Bonfire subscribes to a private bug bounty program through [HackerOne.com](https://www.hackerone.com).

Patch Severity & Timing

Bonfire defines the severity of a patch via industry-recognized [Common Vulnerability Scoring System \(CVSS\)](#) scores, which all modern scanning and continuous monitoring systems utilize. The CVSS provides a way to capture the characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

All vulnerabilities will be addressed within reasonable timelines as defined by company procedural commitments.

Low Severity - 0.1 - 3.9

Low severity vulnerabilities are likely to have very little impact on the business, perhaps because they require local system access.

Medium Severity - 4.0 - 6.9

Medium severity vulnerabilities usually require the same local network or user privileges to be exploited.

High Severity - 7.0 - 8.9

High severity vulnerabilities are typically difficult to exploit but could result in escalated privileges, significant data loss, and/or downtime.

Critical Severity - 9.0 - 10.0

Critical severity vulnerabilities likely lead to root level compromise of servers, applications, and other infrastructure components.

Patch Installation

Bonfire uses an automated patch management system that deploys security patches on a regular basis.

Asset Management Policy

This Asset Management Policy is designed to protect customers' data stored on endpoints, including laptops and mobile devices. It details how Bonfire accounts for endpoint information technology assets (e.g. employee computers) and outlines what should be done if assets are lost, destroyed, or otherwise damaged.

Asset Standards

Any new type of asset (e.g. a new computer model) that will be used for Bonfire's operations must be reviewed and approved.

Devices should be configured such that there's reasonable confidence they will last 36 months.

Configuration Standards

When Bonfire purchases the same hardware asset repeatedly, the team should design and implement consistent, secure configuration standards to ensure assets are configured securely and consistently. The standards should be based on the team and role of the Bonfire employee who will be using the asset.

All devices provided by the company should have included in the baseline configuration:

- Apple Business Manager enrollment
- Mobile Device Management (MDM) software (e.g. Jamf Pro)
- Password management software (e.g. 1Password)
- Hard disk encryption (e.g. FileVault) enabled
- Password-protected screensaver that activates automatically after 15 minutes or less
- Host-based Firewall (e.g. OS X's application firewall) enabled
- Antivirus/Anti-malware software
- Other approved security/audit software (e.g. EDR, Compliance audit tooling, etc.)

Variations to the Configuration Standard

Deviations from the standard configuration should be documented and approved by the Bonfire IT and Security team. The IT and Security team should only approve deviations for which there's a valid business need. Deviations will be documented in the company's inventory list and, if applicable, the Bonfire Risk Register.

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.

Software Licensing Guidelines

Bonfire's Vendor Management Policy details the policies for third-party software and services

Technical Support and Maintenance Practices

The IT team is responsible for technical support and handles employee device maintenance.

Support and maintenance requests should conform with all of Bonfire's security policies.

Company maintenance policies are:

- If a device breaks in the first 36 months, the employee will be given a loaner device while the original is repaired
- If an employee leaves the company, his/her device(s) will be wiped and reissued if purchased in the past 18 months; older devices will be added to the loaner pool
- Computers may be replaced when they are 36 months old
- The IT team should handle device exceptions that do not meet these policies

Configuration Management Guidelines

Bonfire employees are responsible for installing critical firmware, OS and software updates on the assets they use.

The IT Team is responsible for installing firmware and software updates on communal assets (e.g. meeting rooms, office displays, etc.).

Asset Inventory Practices

The Bonfire IT Team is tasked with maintaining a list of all company-owned assets.

Employees must immediately report lost, stolen, or damaged devices to the IT Team, which will then remotely lock down the missing asset as soon as possible.

Asset Disposal Guidelines

Whenever possible, Bonfire refurbishes and reissues assets. If an asset will not be reused internally, the Bonfire IT team must perform a secure wipe to delete all company and customer data and invalidate access credentials before disposing of it.

Policy Exceptions

Any exception to the policy must be approved in advance and may be placed on the risk register for monitoring and periodic review.

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.