

Bonfire Data Protection Policy

Bonfire Interactive Ltd. | Confidential

Table of Contents

Introduction	4
Data Protection Policy	4
Data Classification Policy	5
Public	6
Internal	6
Confidential	6
Data Encryption Policy	7
Data Encryption	7
AWS Data Encryption	7
Data in Transit	7
Data at Rest	8
Encryption Standards	8
Bonfire Encryption Key Creation & Storage Standards	8
Internal Data Access Policy	8
Employee Access Rules	9
Employee Access Logging	9
Access Keys and Passwords	9
Acceptable Access of Customer Account / Data	9
Exportation of Data	10
Employee Non-Disclosure Agreement (NDA)	10
Contractor Access	10
Data Retention Policy	10
Data Destruction Policy	11
Types of Sensitive Data	11
Electronic Documents	11
Physical Documents	11
Electronic Data	11
Electronic Back-ups	11
Methods of Destruction	12
Electronic Destruction	12
Physical Destruction	12
Authorized Destruction	12
Purging Local Systems	12
Upon Customer Request	12
After System Migration	12
Existence of Meta-Data	12
Hardware Decommissioning	13
EU GDPR Policy	13
Collection of Personal Data	13
What We Collect	13
Data Processor and Data Controller	13

Protection of Personal Data	14
Data Protection by Design	14
Data Protection by Default.....	14
Testing of Data Protection	14
Personal Data Management.....	14
Right of Data Access	14
Right of Rectification	14
Right to be Forgotten	15
Exercising Rights.....	15
Personal Data Breach Notification.....	15
Backup Policy	15
Data Types.....	15
Database	15
Documents and Files	15
Backup Frequency	15
Redundancy	16
Testing.....	16
Endpoint Backups.....	16
Policy Exceptions	16

Introduction

This policy refers to all Bonfire data including that which is collected from employees, users, customers, vendors, or other parties that provide information to Bonfire. Bonfire employees must follow this policy. Contractors, consultants, partners and any other external entities are also covered. Generally, our policy refers to anyone we collaborate with or who acts on our behalf and may need access to Bonfire data.

Data Protection Policy

As part of our operations, we obtain and process information, some of which can be used to identify individuals (personally identifiable information, or PII).

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

The data will be:

- Accurate and kept up to date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and ethical boundaries
- Protected against any unauthorized or illegal access by internal and external parties

The data will not be:

- Communicated informally
- Stored for more than the amount of time specified in our Terms of Service, Privacy Policy, customer contracts, or other binding agreements
- Downloaded to unapproved devices
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data, Bonfire has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Have provisions in cases of lost, corrupted, or compromised data
- Allow people to request that we modify, erase, reduce, or correct data contained in our databases within legal guidelines specified by company policies or law-enforcement agencies

To exercise data protection, we're committed to:

- Restrict and monitor access to sensitive data

- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish procedures for reporting privacy breaches or data misuse
- Establish data protection practices (document shredding, data encryption, frequent backups, access authorization etc.)

Data Classification Policy

In order to effectively secure Bonfire's data, staff must have a shared vocabulary to describe the data and the corresponding protection it requires. This policy describes how company data may be classified and the levels of protection required for each classification.

This data classification standard and policy applies to all Bonfire data, both physical and electronic.

All Bonfire information and all information entrusted to Bonfire from third parties falls into one of three classifications, in order of increasing sensitivity.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Bonfire.	Press releases Public website
Internal	Access to internal information is approved by management and is protected from external access.	Internal memos Design documents Product specifications Correspondences
Confidential	Information collected and used by Bonfire to operate the business. Bonfire must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	Legal documents Contractual agreements Employee PII Employee salaries Customer operating data Customer PII Call recordings

		Risks Bonfire financial information Anything subject to a confidentiality agreement with a customer
--	--	--

Public

Public data is information that may be disclosed to any person regardless of their affiliation with Bonfire. The “public” classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to any data that does not require any level of protection from disclosure.

While it might be necessary to protect original (source) documents from unauthorized modification, public data may be shared with a broad audience both within and outside Bonfire, and no steps need be taken to prevent its distribution.

Internal

Internal data is information that is potentially sensitive and should not be shared with the public. Internal data generally should not be disclosed outside of Bonfire without the permission of Bonfire management. Unauthorized access has the potential to influence Bonfire’s operational effectiveness, cause an important Financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence.

Confidential

Confidential data is information that, if made available to unauthorized parties, might adversely affect Bonfire or its customers. This information is to be protected against unauthorized disclosure or modification and might be limited to executives, HR, and legal parties employed by or under contract with Bonfire.

This classification also includes customer data and data that Bonfire is required to keep confidential, either by law or under a confidentiality agreement with non-customer third parties, such as vendors. Customer data should be used only when necessary for business purposes with the permission of the customer.

All confidential data should be used only by pre-authorized parties and should be protected both when it is in use and when it is being stored, processed, or transmitted.

Unauthorized access has the potential to influence Bonfire’s operational effectiveness, violate contractual confidentiality agreements, initiate a security incident, or cause a major drop in employee, customer, and industry confidence.

Data Encryption Policy

This policy provides guidance to limit encryption to those algorithms that have received substantial public review and have been proven to work effectively.

Additionally, this policy provides Bonfire encryption standards and best practices to ensure that Bonfire consistently follows industry standards for Encryption and Key Management.

This policy and standard applies to all Bonfire employees, contractors, and third party vendors when sensitive data, such as customer data, Bonfire secrets and PII, are in scope.

Data Encryption

- All sensitive data in transit and at rest must be encrypted using strong, industry-recognized algorithms.
- Bonfire maintains approved encryption algorithm standards. These internal standards are reviewed and subject to change when significant changes to encryption standards within the security industry change.
- Bonfire will not engage in “roll-your-own” encryption, algorithms, or practices and will not use “security through obscurity” as a sole control within production infrastructure or applications.
- All Bonfire-owned, employee-utilized computers are to have full disk encryption enabled at all times, as these devices are expected to interact with Bonfire resources, infrastructure and/or client data while performing Bonfire business.
- All Bonfire-owned wireless networks, including both corporate and guest networks, are to encrypt corporate office data in transit using WPA2-AES encryption.

AWS Data Encryption

Bonfire uses AWS resources to store and encrypt sensitive data. To keep data encrypted at rest, Bonfire ensures that all new and existing resources use Amazon server-side encryption. By default, AWS encryption uses AWS-owned or AWS-managed keys stored in KMS or S3.

Amazon server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt Bonfire data.

Bonfire engineers are required to ensure that Amazon resources are correctly configured to use AWS server-side encryption in a secure manner following Amazon recommendations.

Data in Transit

- The minimum acceptable TLS standard in use by the company is TLS v1.2.

- All Bonfire public web properties, applicable infrastructure components and applications using TLS, IPSEC and SSH to facilitate the encryption of data in transit over open, public networks, must have certificates signed by a known, trusted provider.
- Bonfire servers are to be configured to switch any unencrypted requests over to an encrypted connection.

Data at Rest

- All Confidential data as defined by the Data Classification Policy must be encrypted at rest using industry recommended encryption algorithms and best practices.

Encryption Standards

The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Ciphers in use must meet or exceed the set defined as “AES-compatible” according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2 , or any superseding documents according to the date of implementation.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to the date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

Bonfire Encryption Key Creation & Storage Standards

Encryption Keys generated, stored, and managed by Bonfire

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Transmission of encryption keys must be done using secure communication systems.
- Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

Internal Data Access Policy

This document details Bonfire’s internal data access policy for managing employee access to confidential customer information. The document serves as an internal guide for Bonfire staff in managing access to sensitive customer data.

The following items comprise the policies and processes that govern Bonfire employees' access to confidential customer data.

Employee Access Rules

Employees of Bonfire have specific user accounts for the production systems (i.e. databases and file systems on servers) that comprise the software service. These user accounts have associated permissions that govern the user's access to confidential customer data. Employees are prohibited from sharing account credentials with others.

By default, employees have no access to confidential data; only employees directly related to the activities detailed below ('Acceptable Access') are granted access rights. Such access is granted on a least privilege/need to know basis. In the event of an employee ceasing employment with Bonfire, his or her user accounts are immediately suspended.

Improper use of an employee user account is grounds for immediate termination of employment and may result in additional legal action (subject to the employment agreement and non-disclosure agreement).

Employee Access Logging

All employee access to confidential data is to be logged.

Access Keys and Passwords

All access keys and passwords are securely stored in a password management system. Only senior technical staff have access to 'root' accounts for production systems.

Acceptable Access of Customer Account / Data

All employee access to confidential data is limited to the following activities:

- Helping a customer resolve an issue (e.g. answering a support question, troubleshooting a potential bug, checking something by request, etc.);
- Updating a record at a customer's request (e.g. changing a user's email address for them, correcting an incorrectly inputted project parameter, etc.);
- Performing system maintenance (e.g. migrating the database to a new schema during a major update, regular data back-ups, etc.);
- Performing system monitoring and usage analysis (routine monitoring of key system components, monitoring of submission flow during a project close, analysis of usage patterns for possible feature improvements, etc.);
- Periodic data aggregation for reports (e.g. providing usage statistics and reports to customer);
- Anonymized usage information gathering for product development purposes (e.g. analyzing how users on aggregate use a particular feature);

- Other types of access when explicitly requested by customers.

Employees in roles that don't include the above activities do not have access to any systems containing confidential customer data.

Exportation of Data

Employees are restricted from exporting the data from the production systems or backup systems, except in the following cases:

- If a local copy of the customer's dataset is required for debugging purposes. This exportation must be approved by a senior technical executive in advance, and the local data securely deleted immediately upon task completion;
- Anonymized data to be used in testing and/or development. Prior to use, the data must be purged of all identifying information (user accounts, supplier names, documents, etc.) and is subject to prior review and approval by a senior technical executive.

During server migrations or system backups. The local data must be securely deleted immediately upon task completion.

Employee Non-Disclosure Agreement (NDA)

All Bonfire employees are bound by an NDA upon hire. Bonfire's NDA stipulates that customer data is confidential and to be treated with the same regard as Bonfire's own confidential data. No employee is authorized to access any of Bonfire's systems until (1) the NDA is signed and filed, and (2) after the employee's specified start date.

Contractor Access

Any contractor or consultant employed by Bonfire is subject to the same policies and restrictions detailed for staff members.

Data Retention Policy

All Bonfire data is backed up indefinitely. Bonfire will keep data for as long as it remains necessary for the identified purpose or as required by law, which may extend beyond the termination of customer contracts. Bonfire may retain certain data as necessary to prevent fraud or future abuse, or for legitimate business purposes, such as analysis of aggregated, non-personally identifiable data, account recovery, or if required by law. All retained Personal Information will remain subject to the terms the Bonfire Privacy Policy which can be found at <https://gobonfire.com/privacy-policy>.

Data Destruction Policy

Bonfire's Data Destruction Policy describes how customer data is deleted in connection with the cancellation or termination of a Bonfire account.

This policy applies to all data collected by Bonfire except:

- data that resides in any Bonfire product or service not covered by this policy
- data that resides in third-party services managed and hosted by third parties, with the exception of the company's infrastructure provider
- data that resides in Bonfire products or services that are in beta, testing, or an early access program

By default, a customer's data is stored for the duration of their contract with Bonfire. The data may be deleted within one quarter after the contract ends, at the latest, with the exception of data that is required to establish proof of a right or a contract, which will be stored for the duration provided by enforceable law.

Once deleted, a user's data cannot be restored.

Bonfire may provide the option for customers to delete data after their subscription ends. This request must be made by the customer, and Bonfire may require additional ID verification.

Types of Sensitive Data

Electronic Documents

Includes all client files uploaded into Bonfire, and their derivatives (e.g. our intermediate document format). Includes all exported reports and summary files that remain on Bonfire systems.

Physical Documents

Includes all physical artifacts Electronic Documents that Bonfire has exported to a physical medium (i.e. paper) for internal purposes.

Electronic Data

Includes all client data stored in Bonfire's database(s) for the customer.

Electronic Back-ups

Includes all back-ups of Electronic Documents and Electronic Data. Bonfire preserves multiple physically disparate concurrent back-up systems.

Methods of Destruction

Electronic Destruction

All digital assets are securely destroyed with Unix **srm** utility with a minimum of 35 passes. This is consistent with DoD 5220.22-M clearing process. Note that due to the multi-tenant nature of the application, destruction of customer data does not imply clearing of the entire physical storage device.

Physical Destruction

All physical assets destroyed with cross-shredding and using a secure disposal service (NAID certified) for protected removal of the paper.

Authorized Destruction

Data will only be destroyed only in the following authorized cases. All data destruction activities are logged and audited by Bonfire.

Purging Local Systems

From time to time, sensitive customer data is mirrored onto local systems for troubleshooting or maintenance purposes. All sensitive data is destroyed locally immediately upon task completion.

Upon Customer Request

When explicitly requested by the customer, and authorized by the customer's Primary Contact in writing, Bonfire will destroy the specified data as requested.

After System Migration

If Bonfire is migrating the customer data to a new system / server, all the data on the old system / server is destroyed and the hard drives reformatted as defined by Electronic Destruction.

Existence of Meta-Data

After deletion of customer data, meta-data relating to customer data may persist. Any such data is anonymized, aggregated and non-identifiable. Bonfire may use such information to improve performance of the application.

Under no circumstances will such meta-data include personally identifiable information, specific financial information or sensitive data.

Hardware Decommissioning

When production hardware containing customer data is decommissioned, data on the hardware is destroyed. This does not imply that all instances of such data is destroyed, only that the instances of data on the hardware is destroyed prior to its disposal.

Bonfire uses data centers that commit to best practices for data destruction in this scenario – following standards outlined in DoD 5220.22-M, NIST 800-88 or similar for sanitization of data.

EU GDPR Policy

The European Union General Data Privacy Regulation provides data protection and privacy for individuals in the European Union. Bonfire is committed to complying with the GDPR.

This document provides an overview of Bonfires commitments and procedures relating to the GDPR. The complete details of Bonfire's handling of GDPR and privacy in general may be found in our Privacy Policy.

Collection of Personal Data

What We Collect

Bonfire collects a limited set of personal data, as necessary to carry out the application's functions. The personal data collected is minimal and is generally used for the purpose of identifying and/or communicating with users within our system. Personal data may include:

- Name
- Email address
- Phone number
- Profile picture (optional)

Additionally, information that may identify a person, such as IP addresses and user IDs, may be collected.

Our Privacy Policy gives additional details of the personal data we collect and how it may be processed.

Data Processor and Data Controller

Bonfire operates both as a data controller and a data processor. In the case where data is collected on behalf of a client organization, Bonfire assumes the role of data processor, and requests to exercise data rights should be directed to that organization.

Protection of Personal Data

Bonfire takes the security of all data, including personal data, very seriously. A number of approaches are taken to ensure data is appropriately protected.

Data Protection by Design

Protection of data is an important consideration and included in the design of all Bonfire systems. Data protection and security is an important part of the entire software development lifecycle.

Data Protection by Default

Bonfire treats data as private, and consequently implements the appropriate protections, by default. Data is made accessible only with careful consideration.

Testing of Data Protection

Bonfire regularly tests the integrity of data protection mechanisms, such testing includes code review, testing of new features and bug fixes, as well as general regression and integration testing.

Security policies, including those which may impact the protection of personal data, are reviewed on a regular basis.

Personal Data Management

The GDPR offers several rights to data subjects regarding their personal data. Bonfire will honor these rights.

The following sections provide detail on some of these rights and how they may be exercised.

Right of Data Access

Data subjects have the right to know if Bonfire processes any personal data concerning them, where it was collected from and for what purpose, and to whom it may have been disclosed. Upon request, Bonfire will disclose to a user this information.

Additionally, a data subject may request a copy of this data. Bonfire will provide this on request

Right of Rectification

Data subjects have the right to the correction of inaccurate personal data concerning them. Bonfire will provide this rectification without undue delay upon request.

Right to be Forgotten

Data subjects have the right to have their personal data erased where there is no legal obligation for Bonfire to retain it. Bonfire will honor these requests.

Exercising Rights

Requests to exercise rights under the GDPR may be directed to support@gobonfire.com. Please note that Bonfire is required by the GDPR to gain proof of identity from the data subject before giving effect to these rights. Bonfire will comply with requests within 30 days.

Personal Data Breach Notification

In the event of a personal data breach, Bonfire will disclose details of the breach to those affected in a manner that is appropriate to the nature of the breach. Please refer to our Support and Incident Management Policy and Data Processing Agreement for details.

Backup Policy

This document provides an overview on Bonfire's policies and processes regarding the backup of data. All original (non-derived) customer data on infrastructure operated by Bonfire should be backed up.

Data Types

Database

Databases are backed up via two mechanisms; the first is real time replication to a secondary database (under a master-slave configuration) in a geographically distinct location, the second is a periodic dump of the database.

Documents and Files

Upon upload, all documents and files are immediately placed in multiple redundancy storage.

Backup Frequency

The frequency of data backup depends on the data type.

Data Type	Frequency	Retention
Database – replication	Continuous	Permanent
Database – dump	Hourly, Daily, Weekly, Monthly	Rolling – keep last dump for each frequency

		Hour: 48 Day: 31 Week: 26 Month: 12
Documents and Files	Continuous	Permanent

Redundancy

All backup data is stored in a separate location from its source. Backup data is stored in a geographically redundant nature, meaning that multiple copies of the backup data are stored in distinct locations to safeguard against storage failure including facility wide failure.

Testing

Backups and restoration mechanisms are periodically tested by the Engineering team.

Endpoint Backups

Bonfire does not maintain backups of employee endpoints (laptops or computers). Key tools, documents, and work products are expected to be stored on approved cloud services and shared drives so that creating and maintaining backups of employee endpoints is not necessary.

Policy Exceptions

Any exception to the Data Protection Policy must be approved by the CTO in advance and placed on a risk register for monitoring and periodic review.