BIZIMPLY

SECURITY WHITE PAPER

Change History

Version Number	Date published	Author	Summary of changes
1.0	March 2022	Adam Morrissey & Katie Whiteside	Completion of version 1.0
1.1	21st March 2024	Adam Morrissey	Update to version 1.1, inclusion of ISO27001 controls and practices.
1.2	1st May 2024	Adam Morrissey	Update to version 1.2, updated key terms

Introduction

As businesses become more dependent on using and storing data in a digital format, keeping employee and customer data safe and secure becomes a higher priority for everyone. As digital threats become more prevalent, ensuring data security across all aspects of our business is at the highest standard is more important than ever. Bizimply is committed to ensuring all data is kept safe and secure for our customers, shareholders, partners and employees.

This document will provide you with more information on our Information Security practices and controls, both internally as a company and within our product. You can use the information in this document to complete a Data Protection Impact Assessment (DPIA) when using Bizimply as a data processor.

The General Data Protection Regulation (GDPR)

Bizimply is a data processor under the GDPR. The GDPR applies to companies in the EU as well as the United Kingdom as all companies that process or store the personal data of EU citizens, regardless of their location. Bizimply regularly reviews the GDPR requirements and updates our privacy and security practices to ensure data processor compliance with GDPR at all times.

These practices include:

- Training employees on security and privacy practices
- Conducting privacy impact assessments
- Maintaining records of processing activities

BIZIMPLY

Data Protection Officer

Bizimply contracts an external security contractor and DPO who provides information security advice, conducts an annual penetration test, and perimeter network assessments and conducts annual GDPR & Information Security audits.

Internal Bizimply Security

Human Resources Security

Before employment, we have a pre-employment screening process that involves checks such as confirmation of claimed academic and professional qualifications and identity checks. The functions and duties of staff are outlined in their contracts as well as disciplinary guidelines, termination of contract and the return of property and assets. We provide appropriate information security awareness training to our employees as deemed relevant for the job function as part of their onboarding. Training on policies and procedures is also provided to employees and a formal disciplinary process is in place to handle policy violations. Bizimply has a formal joiner, mover and leaver process to assign and remove user access rights.

Physical and environmental security

We operate access controls to all our assigned offices. These controls include employee access badges & CCTV. Security controls have been defined for third parties/visitors in the office i.e. they are supervised and all visits are logged. Bizimply also has a clear desk policy for office and remote work.

Asset management

We maintain an asset register and also have procedures to assign asset ownership at the time the asset is created or transferred within the organisation. As part of the termination process, we have procedures to ensure that the company's assets are returned and wiped of all company and sensitive data.

All Bizimply staff have mobile device management (MDM) software installed on all company devices for remote device management. All devices have the latest antivirus and VPN software installed to enhance security for employees who work remotely.

We have information classification guidelines to assign classification levels to data and determine the appropriate protection level. We have procedures in place for the secure destruction and disposal of media and data.

BIZIMPLY

Password Policy

Bizimply has a stringent password policy to provide clear guidance and present best practices for the creation of strong passwords, the management and protection of those passwords, and the frequency of change. All passwords are required to be a minimum of 9 characters in length and contain both upper and lower-case letters, numbers and at least 1 special character. All employees are required to use a nominated password manager for all company-related user access.

Staff Training

All staff receive regular information security awareness training including initial security awareness training upon joining Bizimply. This includes data protection requirements & responsibilities, Managing Online Risks, Protecting Information, Safe Device Use and Keeping safe online. Staff are also provided with copies of relevant information security policies to aid in the upkeep of training and security standards

All staff have antivirus and a VPN installed on company hardware. System and security patches are enabled and run on a routine basis on all endpoints. All staff are obliged to use VPNs when working outside our main office.

Security Breaches

Customers will be notified within 72 hours of a security breach relating to their data unless we can demonstrate that the personal data breach is 'unlikely to result in a risk to the rights and freedoms of natural persons'.

Security Compliance and Certification

Bizimply actively works with security in mind from the development of the Bizimply application to the use and regulations of using company-owned devices. Bizimply is ISO27001 certified and continuously strives to achieve greater security standards for its product, customers and staff and also in full compliance with the GDPR. We also work with an external data protection officer (DPO) who provides information security advice when needed and provides penetration testing and annual security compliance audits.

BIZIMPLY

Product Security – Bizimply Web App

What information can we collect about you?

The GDPR expands and clarifies the concept of personal data. While the basic concept of personal data largely remains the same, the GDPR makes it clear that location data and online identifiers, such as IP addresses, are considered personal data. The GDPR also expands the concept of sensitive personal data to include genetic data and biometric data.

This is the list of the information gathered by an employer and held about users in the Bizimply App. This information covers both the GDPR personal and sensitive data categories.

Basic Information	Suffix or Title; First Name; Last Name;
Contact Information	Email Address; Home Address; Mobile Number; Home Number; Emergency Contact;
Profile Information	Date of Birth; Job Title; Passport Expiry; Visa Expiry; Gender; Ethnicity; Nationality; Marital Status; Profile Picture; References; Employment History; Education; Payroll information; Training records; Time off records; Sickness records;
Financial Information	Payroll Information; PPS Number; Bank Name; Branch Name; Sort Code; Account Number; Account Holder Name; BIC/Swift Code; IBAN; Building Society Number;
Newsletter Information	When signing up to a newsletter, we take: First Name;

	Last Name; Email Address; When signing up for a product demo, we take; First Name; Last Name; Email; Company Name; Phone Number;
Technical Information	Web Pages Viewed; Website Visits; Web Browser used; Web Browser version used; Web Sessions; Stripe ID; Device Used; Device Name; Device Operating System Version; Device App version; Number of sessions; Other in-app messages; User Photos; User Videos; Files & Documents; Device or other IDs;
Location Data	Approximate GPS location; Precise GPS location;
Any Other Information	Doctors notes; Medical Records; Training Records;

Bizimply's sub-processors, Vendors & Suppliers

A sub-processor is a third-party company that Bizimply uses to process customer-related data. We have included the names of these companies within our terms of business. This can be found here. When Bizimply chooses a new sub-processor, vendor or supplier to use to help in operations

related to the processing of customer-related data, supplier due diligence is carried out before the onboarding and rollout of the new service or tool.

This process includes choosing the right vendor/supplier to aid in a specific function and carrying out a security review of the chosen vendor/supplier. This review includes the desired vendor/supplier completing a due diligence questionnaire which highlights the security practices within the company such as if they have any business certifications, administrative safeguards and technical & physical safeguards.
Also carried out is an agreement review which covers certain requirements such as but not limited to:

- Relevant policies
- Data protection agreement in place
- Legal and regulatory requirements
- Intellectual property ownership identified
- Supply chain management
- Right to audit
- Assurance of employee training and vetting
- Requirements for agreement termination

Roles and Permissions in the Bizimply Web App

Within the Bizimply application, access permissions and roles are highly customisable and allow the creation of specialised roles with specialised permissions even for a specific person within your business thus allowing access to only the information required for their role.

Admins

Admins have full access to all areas within Bizimply. They can control all settings within an account. They can view all locations created within the account and can access all employees' information such as personal details, time off records, payroll information and employees' permission levels. Admins can also access the plans and billing section of the account.

Managers

Managers have access on a more local level. With full permissions, they can access the same level of information for employees as admins but only within locations that they have access to. They can also access attendance records, timecards, schedules, reports and sales information. Managers don't have access to any account settings.

Employees

Employees only have access to their information within their employee portal and can request holidays if that feature has been activated within an account.

Data Back-Ups

All customer data is stored and backed up in Amazon Web Services (AWS) servers in the EU-WEST-1 data centre. All backups are encrypted and automated. Snapshots of the database are taken every day and backups are kept up to 35 days. Audit logs on AWS capture who has accessed systems, when and what changes were made.

BIZIMPLY

Production Environment

All updates to the Bizimply application are created and tested in a “Staging” environment (An environment that is a replica of the main application but only contains dummy/fake data to support testing of new features) before going live in the main “Production” environment. These updates include security updates, Application updates and infrastructure updates. All employees have unique login IDs when accessing data.

Our Network boundaries are protected by firewalls - AWS security groups and we have an Intrusion Detection System/Intrusion prevention system - Guard duty on AWS. IP addresses trying to connect to Bizimply pass through CloudFront & a load balancer to aid in managing web traffic and increase security. Access to the Bizimply product is conducted over HTTPS. Annual penetration tests of the application and our network perimeter are carried out.

Audit Logs

Our product provides the ability to export audit logs for data changes and also the ability to customise the level of access users can have down to a specific user.

- Updates and changes to employee profiles
- Schedule audit
- Audit of emails sent to employees
- Last edits on profile attributes

Deleting customer data

Cancelled subscription data is automatically deleted 30 days after their churn date. Backups which store the churned customer data will be deleted after 35 days.

ISO 27001

ISO 27001 is an information security standard which was published in 2005 by the International Organization of Standardization (ISO) and also by the International Electrotechnical Commission (IEC). ISO27001 was adopted as a standard at the EU level in 2017. This led to the inclusion of the letters “EN” in “BS EN ISO/IEC 27001:2017” along with the 2017 date. This is a globally recognized standard that outlines the necessities for any organisation's security standards.

Bizimply achieved this certification in December 2023. Having this certification requires Bizimply to be independently audited each year to ensure compliance with the ISO27001 Standard. Bizimply also conducts internal audits of policies and procedures as well as auditing from our external DPO.

BIZIMPLY

Information Security

Bizimply has an information security policy which covers security over many different aspects of the business as a whole. As part of this policy, the following areas are covered

- Classification and handling of information
- Data transfer (digital and physical)
- Security in the office and remote working
- Monitoring and use of information assets
    - Securely working with laptops
    - How laptops are secured
    - The return of assets
    - Using email & the internet
    - Access to information assets

Access Control

All bizimply staff are granted access to only assets that are required to perform their duties. Access to assets is reviewed before being provided to users. Bizimply operates its user accesses on a "least privilege" model, meaning that only the bare minimum access needed for a specific person is granted. Access to assets is subject to review either on a 6-month basis or if an individual's job role has changed. Access to assets must also follow the password policy as a minimum requirement. Access to assets is documented and access is removed from users if they leave the company.

Secure Development

When developing the product, Bizimply follows a secure development life cycle process with the following stages:

1. Requirements gathering and analysis
    a. Security requirements must be identified during this phase
2. Design and architecture
    a. Security controls must be implemented in the design phase.
3. Coding and implementation
    a. Any code that is to be deployed goes through an automated system to identify any security vulnerabilities. If any vulnerabilities are identified, the code is not deployed. OWASP top 10 checks are also in place during the deployment process.
    **OWASP is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.*
4. Testing
    a. All software developed must undergo thorough testing and quality assurance to ensure previously established requirements are met and working as expected.

Testing is conducted in a “Staging” environment before deployment to “Production” (live environment)

5. Deployment
    a. The development and release of any code to the production environment are automated through GitHub and AWS Elastic Beanstalk
6. Maintenance
    a. Bizimply uses a monitoring service which constantly monitors the application for issues or security vulnerabilities.

A yearly audit of the secure development policy is conducted to ensure compliance with the policy but also to ensure compliance with the ISO27001 standard.

Incident Management

Bizimply operates an incident management process that covers formal reporting and response procedures, assessing information security issues, classifying them as Information security incidents and performing of a root cause analysis.

Written/documented information security policies are reviewed & updated on an annual basis by our Information Security Manager and Data Protection Officer. This policy applies to all areas and departments of the business. The primary stages of managing incidents are the following:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

These stages cover the fundamentals of who to report an incident to, documenting the incident, communication both internally and externally if required, responding to the incident and documenting lessons learned to aid in the prevention of it from occurring again in the future. Depending on the severity of the incident, this could lead to following either the Business Continuity Policy or Disaster Recovery Policy.

Business Continuity Procedure

Invoking the Business Continuity procedure can vary between organisations but these are the common factors which may trigger the BCP

- The severity of the incident
- Impact on critical functions
- Unavailability of resources
- Legal and regulatory requirements
- Safety and well-being of personnel
- Activation triggers (Specific circumstances pre-defined to invoke BCP)

As part of this process, a BIA (Business Impact Assessment) is carried out to enact a strategy to keep the affected business area operational during the initial aftermath. This will stay in place until either normal/expected business functions resume or a Disaster Recovery Plan has been completed.

Disaster Recovery Plan

Bizimply uses a DRP to ensure that critical business functions and IT systems can be restored in a timely and effective manner following a disaster or event which disrupts business function. This procedure contains the following steps:

1. Assess the situation
2. Perform a risk assessment
3. Assemble a team
4. Establish and implement a recovery strategy
5. Communication both internally and externally (when required)
6. Monitoring of the situation and recovery strategy
7. Document and learn

These steps are in place to aid in assessing the situation, implementing a plan to recover from a major incident, reviewing the cause of the incident, putting in place changes to resume normal business operations and learning from the incident to help prevent it from happening again in the future.

Encryption

Data at rest is encrypted with AWS KMS (Key management system) which uses AWS-256-GCM encryption. Data in transit such as communication with the web application and API communications are encrypted with TLS 1.2
We also encrypt the database using keys that are managed through AWS Key Management Service (KMS). Only Senior developers have authorised access to our production servers through secure keys.
Bizimply staff's work devices are encrypted and the keys are stored securely within Bizimply's chosen MDM (Mobile Device Management) service.

Security Controls

The Bizimply web application is multi-tenant and separation is done at the application layer in the database. Customers only have access to their information stored within AWS.

- Developers use Security keys
- Encrypted connections
- Application servers are in private subnets, which allows no direct connection from the public internet
- Database servers are in private subnets, which allows no direct connection from the public internet
- Back-ups encrypted
- We use BucketAV anti-virus for scanning uploaded documents/files

- Microsoft Sentinel is used to track and scan log files for security purposes

Customer file uploads

Keeping files that are uploaded to Bizimply secure is as important as keeping any other data within Bizimply safe and secure. The following are measures taken to keep file uploads safe

- Uploaded files that are stored in AWS S3 buckets are encrypted at rest with AES-256
    - *AWS S3 is a service where files such as text documents, images, audio files, and videos are stored in a secure and scalable manner
- Uploaded files are sent to AWS directly from the Timestation app using secure credentials
- All data on the iPad/Timestation app is encrypted at rest
- Uploaded files are read from AWS servers on the Web App via secure credentials
- All uploaded files are served to the Timestation and Web app via HTTPS
- Images stored on the iPad/Timestation app will be deleted after 28 days

Bizimply User Access

Controlling user access to your Bizimply account is highly important and also highly configurable. All features within Bizimply have access permissions that can be tailored to a specific user or a group of users. To aid in controlling access to your account the following has been implemented.

- Continuous incorrect login attempts to an account will result in the user being locked out for a period of time
- User access passwords are never sent via email
- Bizimply offers automatic user logout which can be customised within account settings. This can range from 15 minutes to 24 hours.
- User access is controlled by account admins who can create custom user accesses depending on their needs.

Database Security

- The database has character escaping turned off
- Passwords are stored in a hashed format. Even with direct access to the database, passwords cannot be determined.
- Specific fields within the Bizimply application are encrypted to keep sensitive information safe, such as “Bank Details”

Application Security

- Error reports are automatically emailed to developers

- Secure Sockets Layer (SSL) is used online for all logins and is an option for any accounts using a Custom Domain
- OS (Operating System) and middleware security updates are applied and routinely checked.
- High-strength passwords, 2FA and IP restrictions are used.
- Debugging is only available to registered IP Addresses.
- Data is hosted on AWS so physical access is not applicable.

Hosting

- The servers are in a highly secure location.
- Physical access to servers is limited.
- Digital access to production servers is limited internally
- A firewall prevents access from unauthorized locations

Testing and Awareness

- We monitor general internet security threats and ensure updates and hotfixes are promptly applied.
- External audits are conducted on Bizimply and its web application.
- Microsoft Sentinel is used to automatically detect security threats
- Bizimply uses several different tools which scan daily for security vulnerabilities areas across the business.

BIZIMPLY

Frequently asked questions

Are employees required to use a VPN when accessing the organisation's systems from remote locations?

Yes. All employees are required to use our company VPN when working remotely.

What happens with photos that are taken on the iPad Timestation App?

Photographs are accessible via the Timestation App and web app when photo upload is enabled. They are not available in the camera roll or elsewhere on the iPad/Tablet. Photographs are automatically deleted from the Timestation App within 28 days. If Photo Upload is turned on in the app, photos are stored in Amazon AWS S3 and can be viewed within the Bizimply web app online. Photos stored in AWS S3 are encrypted with AES-256. If photos are uploaded to the Bizimply web app these can be deleted upon request by an account administrator.

Are the photos taken on the timestation app biometric data?

Under GDPR, Biometric data is considered a special category of personal data. The GDPR defines it as *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".*

The timestation app only takes a picture of the individual when they are clocking in or out. The processing of this photo/image is not considered Biometric data. Photographs are only considered to be so when processed through a specific technical means allowing the unique identification or authentication of a natural person. Bizimply does not have the technical means to ID individuals. The identification of individuals clocking in and out is a manual process by the manager or admin of the app.