

Technical Overview

2022



Contents

1.	Introduction.....	1
1.1	Our Team.....	1
1.2	The applications	1
1.3	Our Values - The Three 'S'	1
2.	Infrastructure security	2
2.1	AWS Security Tools	2
2.2	Encryption.....	2
2.3	Backups.....	2
2.4	Tenant Separation	2
2.5	Service Level Agreements	3
2.6	Monitoring and alerts	3
2.7	Logging.....	3
3.	High level infrastructure.....	4
3.1	Database	4
3.2	Scalability and stability	5
3.3	Office security	5
4.	My Digital Architecture	6
4.1	Technology stack.....	6
4.2	Authentication	7
5.	In-app security features.....	8
5.1	In-app security options (My Digital Accounts)	8
5.1.1	Password Policy.....	8
5.1.2	PDF Email protection.....	9
5.1.3	Idle Timeout	9
5.1.4	Multi Factor Authentication	9
5.2	Enhanced security features	9
5.2.1	Single Sign On (SSO) support for Azure Active Directory (AAD).....	10
5.2.2	IP Whitelisting	10
6	API Platform	11
6.1	Admin functions	11
7	Application Development.....	12



7.1	My Digital Software Development Life Cycle (SDLC)	12
7.2	Penetration testing	12
7.3	Web Application Firewall (WAF)	12
7.4	Stress Testing.....	12
7.5	Reporting	12
8	Product Development.....	13
8.1	Public Roadmap	13
9	IT and Operational Security	14
9.1	Cyber security Handbook.....	14
9.2	Corporate password manager	14
9.3	Endpoint security	14
9.4	Device Security	14
9.5	Vulnerability Assessment	14
9.6	Phishing simulation	14
9.7	Training and awareness	14
9.8	Risk Management	15
9.9	Disaster Recovery (DR) and Business Continuity Planning (BCP).....	15
9.10	Email protection	15
9.11	Termination of employment	15
10	Privacy and Compliance	16
10.1	My Digital and GDPR	16
10.2	Data Processing Addendum (DPA).....	16
10.3	Privacy Policy.....	16
11	Accreditations	17



1. Introduction

My Digital manages the data of over 70 clients across the UK recruitment industry, and with this responsibility, we are committed to providing our clients with industry leading security and data protection standards. This document may be modified from time to time and it is the responsibility of the reader to download the latest published version from our website.

1.1 Our Team

My Digital's information security approach is guided by our Technology governance team comprising of the CTO, Chief Architect, Cloud Admin, Infrastructure, Ops, Security, Engineering and SysAdmin teams.

We align our processes to the Information Security Management Systems framework as set out by the ISO 27001 Standards.

1.2 The applications

This document covers all the applications owned by My Digital including My Digital Accounts, My Digital Timesheets and My Digital Bridge.

1.3 Our Values - The Three 'S'

Our Infrastructure and software application is built on Three 'S' that we consider as our pillars - Security, Stability and Scalability.

2. Infrastructure security

We host our applications in AWS which allows us to leave the availability and physical security of the servers to AWS under the [shared responsibility model](#). Our data is hosted in Dublin (EU-West-1) and backed up to London (EU-West-2). In both the regions, we operate across multiple availability zones allowing us to continue without interruption should an availability zone go offline.

Following the AWS best practices, our network is separated into public and private subnets.

2.1 AWS Security Tools

We have deployed a number of AWS services to assist in the prevention and detection of security events

- A Web Application Firewall (**WAF**) is in place for web application and API against common OWASP defined attacks
- **GuardDuty** is used to detect for malicious activity and to deliver detailed security findings and recommendations.
- **Security Hub** is used to benchmark our environment against both the *CIS AWS Foundations Benchmark* and *AWS Foundational Security Best Practices* frameworks. We keep monitoring and following the recommended best practices.

S3 buckets are protected with VPC endpoints, meaning this can be accessible only within the AWS network OR from the internal office network.

All databases, EC2 and other AWS services (e.g., Lambda) are hosted in a private subnet to avoid external attacks and any access to the AWS services is only through a site-to-site VPN established between our internal network and AWS. This will restrict user access from any other unknown/home network.

2.2 Encryption

All data in rest are encrypted using AWS KMS. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2. All data is encrypted in transit using a minimum of TLS 1.2.

2.3 Backups

All client data is backed up regularly. The RDS data is backed up every 5 minutes within the primary region and every 24 hours to the secondary region. S3 data is replicated across regions instantly.

2.4 Tenant Separation

Our applications are multi-tenant with logical separation between clients. This is done using a unique key on each database object denoting the client. This ensures that data cannot be viewed across logins and is heavily tested during penetration testing.

2.5 Service Level Agreements

Please refer to our Terms and Conditions [page](#) for details of our SLA agreements.

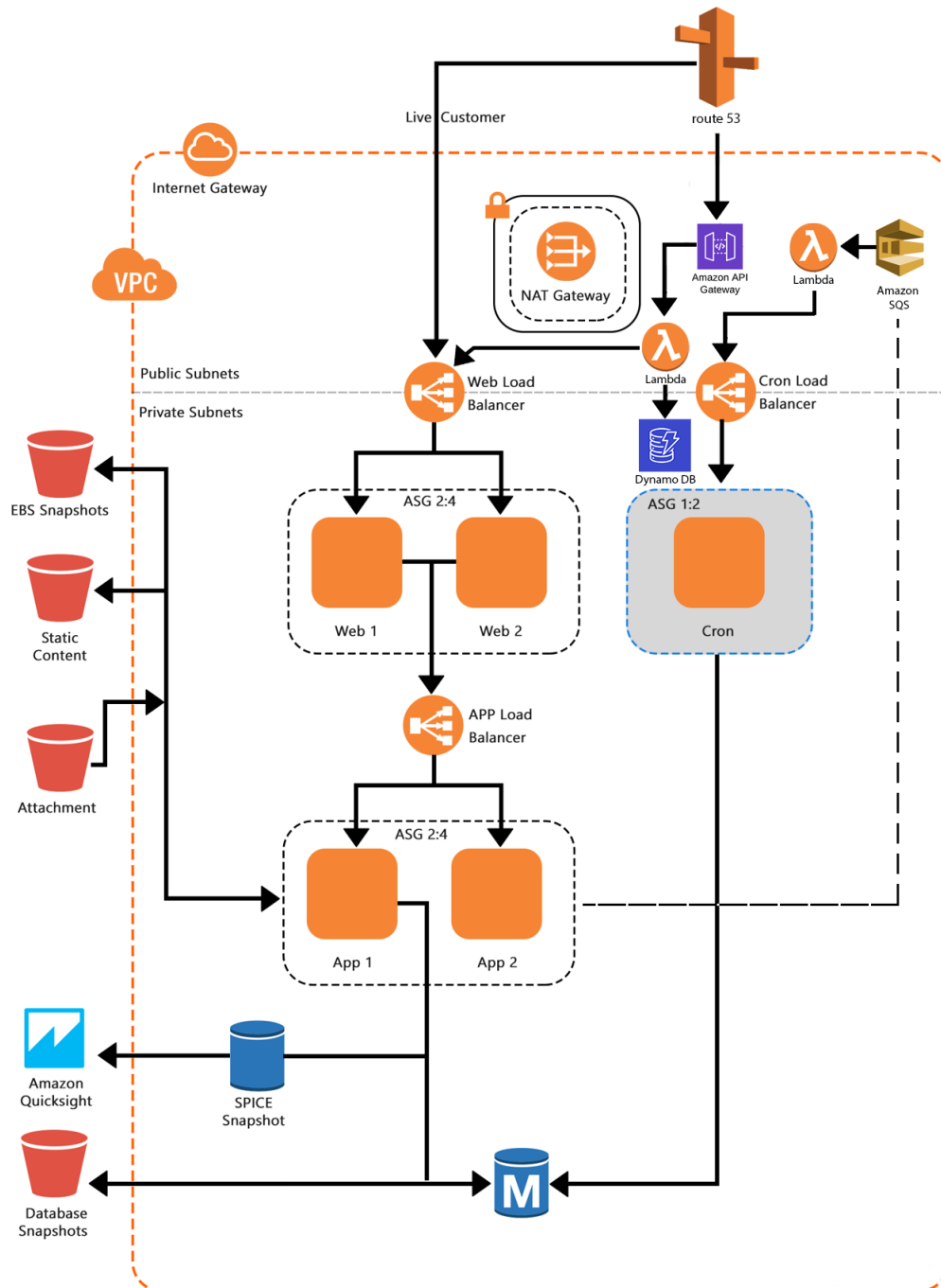
2.6 Monitoring and alerts

My Digital utilises several AWS services to monitor performance and security and use alerts to notify us of anything that could potentially become a problem.

2.7 Logging

All services utilised in AWS have enhanced logging enabled to allow us to perform thorough root cause analysis in the event of any failures.

Below is a high level overview of My Digitals AWS infrastructure. This is similar across the three environments of Gate1 (QA), Staging (UAT) and Production.



Our databases are RDS (MySQL) services with multi-AZ compatibility enabled. This RDS database is a fully managed service and provides the flexibility to operate and scale easily. Multi-AZ make sure high availability with automatic database failover.

3.2 Scalability and stability

Auto scaling groups are deployed for the web and app service layers. This allows the application to scale in a responsive manner when demand increases or decreases. The use of Lambda functions also allows the application to scale several background tasks exponentially.

3.3 Office security

Our UK and India offices both undergo bi-annual audits which consider the physical security of our offices. Both offices have door codes or fob access only and the server rooms are accessible on through a separate key code protected door.

4. My Digital Architecture

My Digital utilises a traditional LAMP (Linux, Apache, MySQL, PHP) stack and follows some of the following architectural patterns: -

Service Oriented Architecture (SOA): MDA architecture contains loosely coupled unit of functionality that are self-contained. Each service will be separated by their own functionality and can be hosted independently. This allows the application to be scaled in a responsive manner.

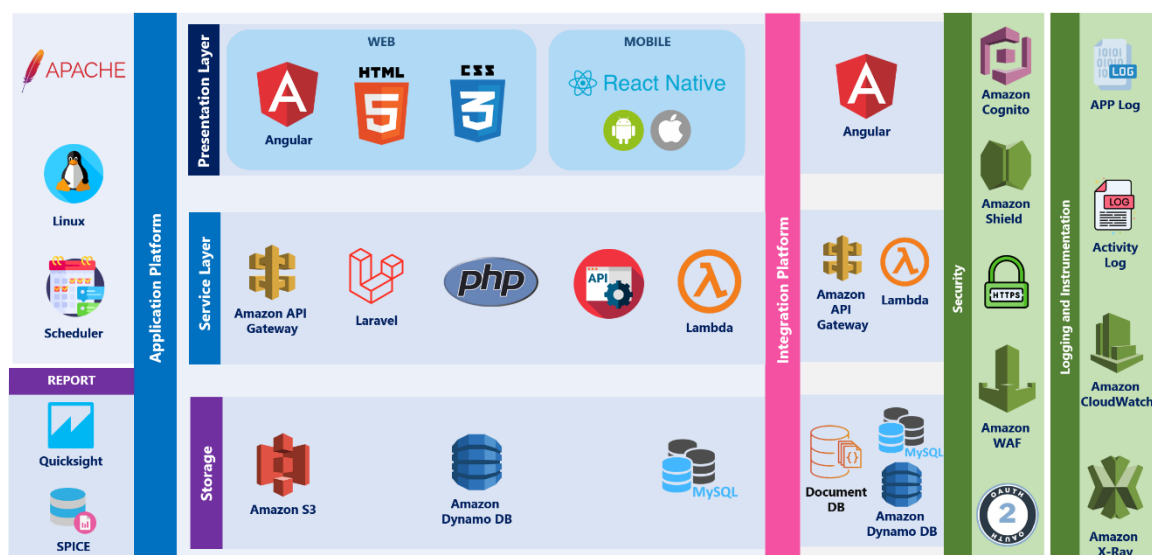
Model View Controller (MVC): MVC is one of the best UI frameworks which separate User interface (View) from UI logic (model and controller). This architecture will be used across all the presentation layers.

Component-based Architecture: Decomposes application design into reusable functional or logical components that expose well-defined communication interfaces

Layered Architecture: Partitions the concerns of the application into separate groups Layers (Presentation, Business Logic, Data Access, etc.).

Shared Nothing (SN): This is a data architecture for distributed data storage in a clustered environment. Data is partitioned in some manner and spread across a set of machines with each machine having sole access, and hence sole responsibility, for the data it holds. Multitenant model of the data base architecture following this pattern.

A high-level representation of our technology stack architecture is shown below



4.1 Technology stack

Our technology stack is the LAMP stack with Angular, HTML, CSS and Node.js.

4.2 Authentication

My Digital uses an OAuth library for authentication and follows an RBAC model for authorisation. We also provide additional security features based on configuration - features like multifactor authentication, IP restriction, strong password policy, and idle timeout. Refer Sec 5, for more information.

4.3 Versions and Patch Management

All our framework and vendor libraries are updated periodically to avoid any library and framework vulnerabilities. The patch manager is one of the AWS system manager's capabilities to keep the system and software up-to-date. We are using this service to keep our infrastructure and software up-to-date.

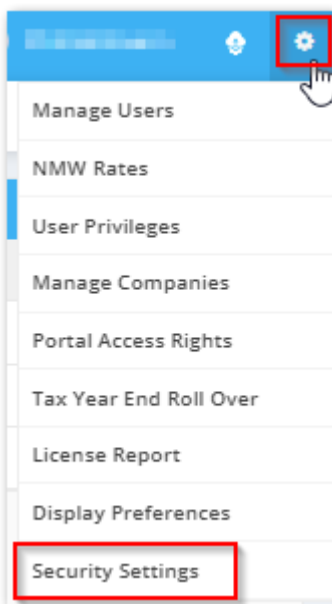
5. In-app security features

As a SaaS provider, My Digital look after the security of the cloud network, the application access security and the protection of your data at rest and in transit.

There are, however, sections of the applications which a client can enable/configure to strengthen their security and meet their internal policy requirement. This section identifies some of the general security recommendations as well as some of the additional security measures you can implement in our applications.

5.1 In-app security options (My Digital Accounts)

Additional security options are available as an Accounting Firm Administrator.



5.1.1 Password Policy

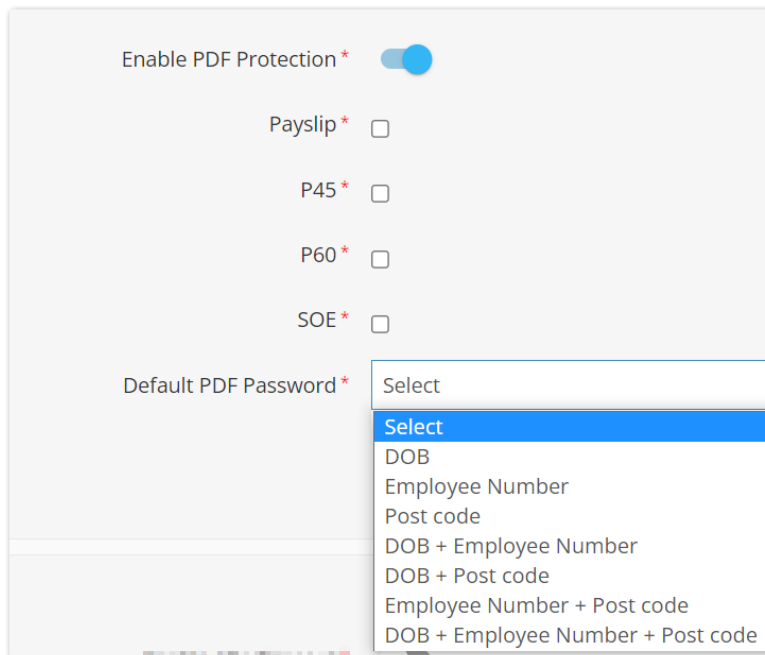
In this section you can apply your company password policy restrictions to the My Digital application. By default, the password must be 8 characters with no password expiration.

A screenshot of the Password Policy configuration form. The form has a light gray background and contains the following fields and controls:

- A toggle switch for "Overwrite MDA Password Policy *" which is currently turned on (blue).
- A text input field for "Password Min Length *" with the value "8".
- A checkbox for "Require at least one uppercase letter from Latin alphabet *" which is currently unchecked.
- A checkbox for "Require at least one lowercase letter from Latin alphabet *" which is currently unchecked.
- A checkbox for "Require at least one non-alphanumeric character *" which is currently unchecked.
- A text input field for "Password Lifetime (days) *" with the value "0".

5.1.2 PDF Email protection

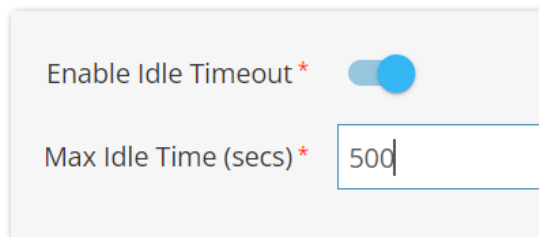
My Digital allows for password protection to be applied to various documents within the application using several password settings.



The screenshot shows a settings panel for PDF Email protection. At the top, 'Enable PDF Protection' is a toggle switch that is turned on. Below it are four checkboxes: 'Payslip', 'P45', 'P60', and 'SOE', all of which are currently unchecked. At the bottom, 'Default PDF Password' is a dropdown menu with a 'Select' button. The dropdown is open, showing a list of options: 'Select', 'DOB', 'Employee Number', 'Post code', 'DOB + Employee Number', 'DOB + Post code', 'Employee Number + Post code', and 'DOB + Employee Number + Post code'. The 'Select' option at the top of the list is highlighted in blue.

5.1.3 Idle Timeout

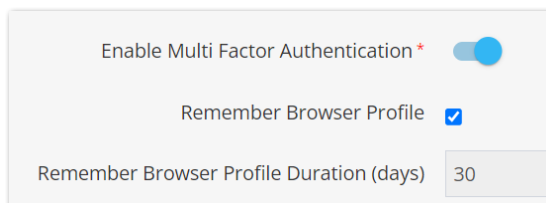
Similar to the password policy, enable this to comply with internal security policies.



The screenshot shows a settings panel for Idle Timeout. 'Enable Idle Timeout' is a toggle switch that is turned on. Below it, 'Max Idle Time (secs)' is a text input field containing the value '500'.

5.1.4 Multi Factor Authentication

My Digital supports MFA for additional security for a client's data.



The screenshot shows a settings panel for Multi Factor Authentication. 'Enable Multi Factor Authentication' is a toggle switch that is turned on. Below it, 'Remember Browser Profile' is a checkbox that is checked. At the bottom, 'Remember Browser Profile Duration (days)' is a text input field containing the value '30'.

For further information on how to set this up please see our help guide [article](#).

5.2 Enhanced security features

For clients on our Quantum Pro package, there are two additional security options available

5.2.1 Single Sign On (SSO) support for Azure Active Directory (AAD)

For those on AAD can use this for their internal users to authenticate rather than using the username and password option. Clients can also configure to allow username and password as a fallback if they would prefer. Please raise a support ticket if you wish to enable this.

5.2.2 IP Whitelisting

For internal users only, application access can be restricted to certain IP addresses (or ranges).

6 API Platform






My Digital has an open API platform allowing for bespoke systems and other applications in the supply chain to take advantage of an integrated ecosystem. APIs are designed and tested based on REST standard. The documentation for our API can be found [here](#) and is available to all client on the Quantum Pro package.

The API allows several features such as: -

- Creating illustrations
- Creating employees
- Creating timesheets
- Updating employee data
- Creating agencies

6.1 Admin functions

The API Admin portal allows requests made through a clients' API key to be viewed.

USER	METHOD	URL	STATUS CODE	TIME	IP ADDRESS
	POST	/vi/crm/people	200	09/05/2022 04:02:04 pm	
-	POST	/vi/login	200	09/05/2022 04:01:58 pm	
	GET	/vi/crm/meta-data	200	09/05/2022 04:01:55 pm	

Clicking on any request shows the request and response data

View Response ×

Request data

```

{
  "role": "CONTRACTOR",
  "gender": "Male",
  "basisNonCumulative": true,
  "title": "Mr",
  "paymentFrequency": "Weekly",
  "employeeNumber": "123456789",
  "bankDetails": {
    "bankCode": "123456",
    "bankName": "ABC BANK",
    "accountNumber": "1234567890123456",
    "accountName": "JOHN DOE",
    "accountType": "BANK_ACCOUNT"
  }
},

```

Response data

```

{
  "message": "People created successfully",
  "data": {
    "externalReference": "123456789",
    "peopleId": "123456789"
  },
  "code": "success"
}

```

7 Application Development

7.1 My Digital Software Development Life Cycle (SDLC)

My Digital follows the OWASP Top 10 methodology and continuously monitors for vulnerabilities as part of our CI/CD pipelines.

All code releases go through a mix of automated and manual test scripts to ensure stable releases.

We continuously monitor defects in releases to ensure robustness in our build processes and future releases.

Our internal security team performs regular static application security testing (SAST) using the OWASP ASVS framework as a guide.

We utilise tools that enable us to check for publicly notified vulnerabilities in all our third-party libraries. Vulnerabilities are assessed and remediated using our patch management policy.

7.2 Penetration testing

In addition to continuous internal security testing, our applications are independently penetration tested on an annual basis. These are marked using CVSS and any critical and high issues are urgently remediated. Medium and Low items are added to the backlog and worked on accordingly.

7.3 Web Application Firewall (WAF)

My Digital utilises WAF as a first line of defence against known attacks. AWS Shield also helps detect and prevent DDOS attacks.

7.4 Stress Testing

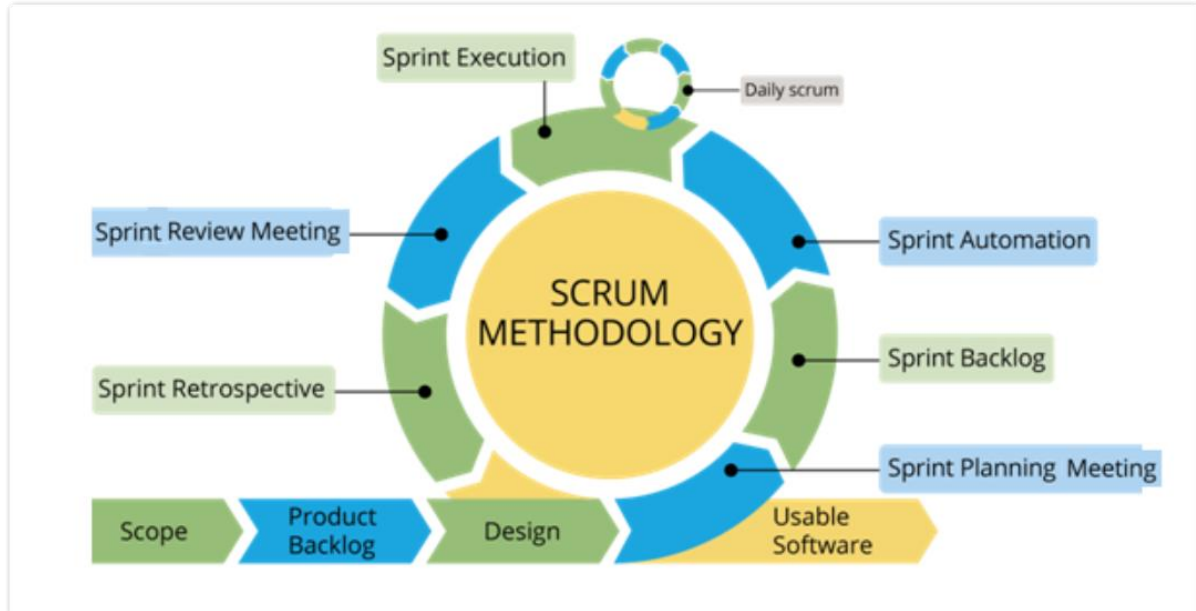
My Digital regularly uses JMeter to stress test the application to ensure we can always support volume which is double the size of our largest client.

7.5 Reporting

There is an extensive customisable reporting solution available to Quantum and Quantum Pro customers utilising AWS QuickSight. This enables clients to write reports based on any data that exists in their organisation.

8 Product Development

My Digital follow agile practices throughout its business. The product development follows SCRUM and currently has 2 - 3 week sprints. Jira is used for the product management along with Roadmunk for the high-level roadmap.



The release process goes through QA and Acceptance Test in Gate1 environment, Regression test in the Staging environment before being released into Production. The releases are done based on release roadmap. My Digital uses Code Commit for the source code repositories and Jenkins for parts of the automated build process.

8.1 Public Roadmap

Our 1-year roadmap is updated quarterly and is available [publicly](#).

9 IT and Operational Security

9.1 Cyber security Handbook

All staff must read and agree to the Cyber security handbook before carrying out any duties. The handbook is reviewed bi-annually and contains, amongst other things

- Password and access management
- Clean desk policy
- Social media usage
- Bring Your Own Device (BYOD)
- Patch management
- Information handling
- Use of cloud/collaboration platforms
- Acceptable use policy

9.2 Corporate password manager

All staff are provided access to 1Password to assist in setting strong, unique passwords.

9.3 Endpoint security

All employee laptops and protected using an approved malware detection tool.

9.4 Device Security

All devices are encrypted using BitLocker, have biometric logins and strong passwords and idle screen timeout is set at 90 seconds.

9.5 Vulnerability Assessment

My Digital works with III Party companies to provide Cyber Security training, support and security consultancy. The service also includes bi-annual Vulnerability Assessment audits of the UK and India offices.

9.6 Phishing simulation

As part of our cyber behaviour training My Digital perform quarterly phishing simulation exercises.

9.7 Training and awareness

All employees undergo Cyber awareness training on their first day, and again on an annual basis. This covers training and assessments on subjects such as physical security, social engineering attacks and GDPR responsibilities.

All our developers are given training on coding best practices as well as study the OWASP Application Security Verification Standard (ASVS) v4 framework. They are tested on both before being given access to our code base.

9.8 Risk Management

My Digital maintains a risk register which is maintained by the senior leadership team and reviewed on a quarterly basis. All items not in an accepted status must contain an action plan on how this risk is going to be reduced.

9.9 Disaster Recovery (DR) and Business Continuity Planning (BCP)

My Digital has a thorough DR plan which is evaluated on a quarterly basis by the Technology team. The DR plan ties in with reference points to the risk management plan. The DR plan has a desktop run through every 6 months with a dry run in a staging environment run annually. Both events have a retrospective with all staff members involved and any improvements are planned.

The BCP ties in very closely with the DR plan and covers off the point at which a disaster is declared, and what everyone's roles are in bringing the business back to its usual activity. This includes supplier and client communication plans and pre-made communication templates.

9.10 Email protection

My Digital uses Microsoft 365 for mail that comes with all the built-in security features and protection from Microsoft. DMARC and SPF records are in place for extra protection.

9.11 Termination of employment

Employees go through a leaving process in the last couple of hours of their employment whereby all equipment assigned to them on the asset register is signed back into the company. All accounts are disabled and the door code to the office changed.

10 Privacy and Compliance

10.1 My Digital and GDPR

MyDigitalAccounts.com is the data controller of personal data relating to its website visitors.

MyDigitalAccounts.com and MyDigitalTimesheets.com is the data processor of all data items submitted through its platform. This is performed on the customers behalf as per the [Terms and Conditions](#). We also use third party processors and some optional third party processors and are identified in [Subprocessors](#)/

10.2 Data Processing Addendum (DPA)

Our Privacy policy together with our Terms and Conditions covers DPA with our customers. Our India entity is a 100% owned subsidiary of the My Digital UK entity. The Data Processing Agreement between our UK and India entities ensures that the Data Protection Act of the UK are enforced.

10.3 Privacy Policy

Our privacy policy can be found on our [website](#).

11 Accreditations

At My Digital, we are proud of our investment into security and information management. In recognition of this we have been awarded the following accreditations: -

Cyber Essentials Plus



Cyber Essentials is a UK Government backed and industry-supported scheme that helps businesses protect themselves against the growing threat of cyberattacks. Cyber Essentials Plus is the highest level of certification offered under the Cyber Essentials Scheme. This audit is performed annually in January.

ISO 27001:2013



This audit is performed annually in February. ISO 27001 is the worldwide security benchmark for Information Security Management Systems (ISMS).