TAX SYSTEMS

Security FAQs

AlphaBridge® & AlphaVAT®

Version 1.2

Contents

1. Version Control

Version	Description of Change	Reviewer	Date
0.1	Initial Version	J Le Roux	17/09/2018
0.2	DevOps section updated	J Le Roux	28/11/2018
0.3	Product Section updated & Review	G Le Brun	12/12/2018
0.4	Reviewed for publication	J Malkin	17/12/2018
1.0	Final sign off	J Malkin	02/01/2019
1.1	Review and updates	J Le Roux	18/03/2019
1.2	Added information for AlphaVAT	G Le Brun	20/08/2019

2. Introduction

We receive multiple requests for information on our company, policies, security and GDPR. This document has been commissioned to address a number of Frequently Asked Questions (FAQs).

Contractually, this is backed up by Service Agreements and Data Processing Agreements (where applicable). If you receive the software to download and run on your premises, Tax Systems is not acting as a sub-processor for you – and will not be processing personal data on your behalf.

In the event of support questions, and where data is required to be exchanged, this will be achieved by encrypting and password protecting the data in transit, with the data maintained securely on encrypted devices while the case is investigated. Once the case is closed, the data is deleted.

The FAQs here are to enable your procurement and security teams to ensure the Supply Chain meets their security and policy requirements.

For additional information, please contact your Account Manager.

3. Company Details

3.1 Tax Systems - Registrations

Registered Office	Magna House, 18-32 London Road, Staines-upon-Thames, TW18 4BP
Website	https://www.taxsystems.com/
Tax Systems Limited	Company Registration number: 04998151
Tax Computer Systems Limited	Company Registration number: 05347048
VAT Number	278491358
Tax Systems Limited	ICO Registration Number: ZA259790
Tax Computer Systems Ltd (UK and Ireland)	ICO Registration Number: ZA189581

4. Certifications

Tax Systems holds Cyber Essentials certification for the whole company and is committed to achieving ISO27001 certification in 2019.

Tax Systems hosts its solutions within Microsoft Azure, with both the primary and secondary datacentres located in the UK (UK South for the primary and UK West for the backup datacentre).

Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud and Singapore MTCS. Further information available at https://azure.microsoft.com/en-gb/overview/trusted-cloud/.

5. Policies & Compliance

Tax Systems is committed to preserving the confidentiality, integrity and availability of all forms of information used by Tax Systems and maintained on behalf of employees, investors, business partners and customers.

The Board of Directors discusses and ratifies, at least annually, the Information Security Charter as it relates to legal and regulatory compliance, privacy protection and information protection.

Policies and procedures are developed, based on industry and vendor best practices, to help administer, manage and protect the information assets under our control. Policies are reviewed at least annually and refined as necessary to keep current with modern threats and technology.

5.1 Policies

Our policies and procedures set standards for our information security controls, some examples being:

- Information Security Charter
- Information Security Policy
- Access Management Policy
- Asset Management Policy
- Computer & Network Management Policy
- Business Continuity Policy
- Acceptable Use Policy
- Remote Access Policy
- Encryption Policy
- Bring Your Own Device Policy

5.2 Supply Chain Compliance

One of our key stated principles is to not knowingly trade with suppliers, customers or any other associate whose activities involve unethical practices. To ensure Tax Systems complies with Supply Chain requirements, we have identified and implemented a number of core policies. Key policies include:

- Bribery Policy
- Modern Slavery Policy
- Diversity and Inclusion Policy
- Corporate and Social Responsibility Policy
- Anti-Money Laundering Policy
- Equal Opportunities Policy
- Confidential Reporting Policy
- Whistleblowing Policy
- Background Check Policy
- Conflicts of Interest Policy

5.3 GDPR Compliance

At Tax Systems, we take data security and privacy seriously and believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights, as such we are committed to maintaining compliance with the GDPR and the Data Protection Act 2018.

Some of the policies and procedures implemented include:

- Data Protection Policy
- Data Deletion and Retention Policy
- Document Control Procedure
- Data Protection Impact Assessment Procedure
- Information Classification Policy
- Data Subject Access Request Policy
- Data Breach Procedure
- Data Processing Agreements *

* We have Data Processing Agreements in place with our sub-processors and, through either a Master Service Agreement (MSA) or individual contracts, with our customers.

For specific questions, please contact us at dpo@taxsystems.com.

5.4 Environmental Compliance

Under our Corporate and Social Responsibility Policy, Tax Systems recognises the global challenge posed by climate change and other environmental issues. The company also recognises its responsibility to reduce the environmental impacts of its business operations.

Tax Systems is committed to reducing its carbon (CO2) emissions and is also committed to managing its direct environmental impacts in a responsible manner.

Another of our core principles is to respect the environment within which we operate, and to expect our employees to mirror this in their working practices.

Our policy is to use recyclable materials where possible, and to favour suppliers that have complementary policies.

5.5 Personnel Checking & Compliance

At Tax Systems, we believe that hiring qualified individuals to fill vacancies contributes to the overall strategic success of the company. Background checks are made as a means of promoting a safe work environment, and protecting the people, property and information of the company.

Tax Systems conducts background checks to:

- Validate a candidate's background and suitability
- Confirm a candidate's right to work
- Ensure we hire reliable employees
- Verify candidates' information for truthfulness and accuracy.
- Screen candidates for any serious convictions

The background checks we conduct include:

- DBS (Disclosure Barring Service) checks
- Right to Work checks
- Reference checks
- Verification checks (e.g. Identity, Employment History, Education)

All employees and contractors have confidentiality agreements as part of their contracts.

Tax Systems follows a consistent and proactive procedure for managing leavers whereby managers and staff have clear steps to follow, security of data and systems are maintained, Tax Systems property are returned and user accounts are disabled.

5.6 Business Continuity (BCP) & Disaster Recovery (DR)

Our objective is to ensure that robust business continuity plans are implemented, tested and reviewed regularly to enable recovery from a major incident or disruptive situation. It is essential that we provide a world-class service to our Customers minimising any disruption in services.

Tax Systems software is backed up securely and in separate secure locations – the software can be made available online via the Portal.

Tax System's has two office locations, geographically separated for Business Continuity and Disaster Recovery.

Core internal systems are provided via Cloud providers and backed up between secure ISO27001 certified data centres

6. Security and Data

Tax Systems take your security seriously and have put policies and processes in place to ensure the data under our control is secure.

6.1 Employee Security Awareness

Security and GDPR awareness sessions are part of the induction process for new starters.

Training sessions on Security Awareness are held once a year as a minimum, and this is a compulsory requirement for all employees. These sessions use an online learning portal that documents the attendance and tests each employee with an exam at the end of the training.

6.2 Penetration Testing

Penetration Testing is completed, at least annually, by an expert third party on our internal and hosted services. The last penetration test was completed by BSI in July 2019.

6.3 Data at Rest

Data at Rest within Tax Systems is stored on encrypted disks and backed up to encrypted media.

All laptops within Tax Systems are encrypted with BitLocker AES-256 or equivalent.

6.4 Anti-Virus

Tax Systems uses Trend anti-virus on internal systems and laptops.

7. Development Process

7.1 Tax Systems Software Development Methodology

The development of software within Tax Systems follows an Agile / SCRUM methodology.

Any enhancement requests or reported and verified issues are analysed and prioritised by our Product Management team before being passed to the Software Engineering team.

7.2 Testing

Our Verification team perform extensive testing on each and every release of our products; this includes both manual and automated testing. Additionally, user acceptance testing is carried out by product experts within the business and releases are signed off prior to the general release.

We do not offer a beta version of the product, and only release once fully tested against specification.

All application upgrades are subject to a full cycle of testing, and no client data is used in our development, test or pre-production environment.

Development, testing, pre-production and production environments are all kept separate.

7.3 Application Control

Production environments for all Tax System applications are separated from the development, testing and pre-production environments.

Developers cannot access any production environments.

7.4 Security during Development

Tax Systems software development security standards cover each stage of the software development lifecycle, which includes security requirement definitions, threat modelling, best practice coding standards and testing.

All code changes are peer-reviewed before being committed to the code-base; additionally, static code analysis is performed which includes reporting on security issues from the SANs Top 25 and OWASP Top 10.

The CTO, Tax Technology Directors, Architects and Senior Software Engineers are involved in controlling and applying these security standards.

7.5 Source Code Version Control

A software versioning and revision control system is used to maintain current and historical versions of source code.

All code changes are peer-reviewed before being committed to the code-base.

8. Hosted Infrastructure Security

8.1 Data Location

Tax Systems hosts its solutions within Microsoft Azure with both the primary and secondary datacentres located in the UK (being UK South and UK West respectively). We do not subcontract the support of our Azure infrastructure; it is under our direct control.

Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud and Singapore MTCS. Further information is available at https://azure.microsoft.com/en-gb/overview/trusted-cloud/.

8.2 Physical Security

Microsoft designs, builds, and operates datacentres in a way that strictly controls physical access to the areas where data is stored. Microsoft understands the importance of protecting your data, and is committed to helping secure the datacentres that contain your data. They have an entire division at Microsoft devoted to designing, building, and operating the physical facilities supporting Azure.

Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacentre resources. Datacentres managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacentre floor.

Please see below for specific details of how the layers of physical security are managed:

Access Request and Approval

You must request access prior to arriving at the datacentre. You are required to provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the datacentres to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the datacentre required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.

Facility's perimeter

On arrival at a datacentre, you are required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacentres, with a security team monitoring the video feeds at all times.

Building entrance

The datacentre entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers routinely patrol the datacentre, and monitor the video feeds from cameras inside the datacentre at all times.

Inside the building

After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the datacentre. If your identity is validated, you can enter only the portion of the datacentre that you have approved access to. You can stay there only for the duration of the time approved.

Datacentre floor

Access is only granted to the floor for which you have been given prior approval. You are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacentre without their knowledge, only approved devices can make their way into the datacentre floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the datacentre floor, you again must pass through full body metal detection screening. To leave the datacentre, you are required to pass through an additional security scan.

8.3 Physical Security Reviews

Periodically, Microsoft conduct physical security reviews of the facilities, to ensure the datacentres properly address Azure security requirements. The datacentre hosting provider personnel do not provide Azure service management. These personnel cannot sign in to Azure systems and do not have physical access to the Azure colocation room and cages.

8.4 Data Bearing Devices

Tax Systems' customer data is encrypted before being stored to disk. Where data is scheduled to be wiped, Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped, they use a destruction process that destroys the disk and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. Microsoft determines the means of disposal according to the asset type. They retain records of the destruction.

8.5 Equipment Disposal

Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling and hardware disposal procedures to ensure that hardware containing your data is not made available to untrusted parties. They use a secure erase approach for hard drives that support it. For hard drives that can't be wiped, Microsoft use a destruction process that destroys the drive and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. Microsoft determines the means of disposal according to the asset type. They retain records of the destruction. All Azure services use approved media storage and disposal management services.

8.6 Compliance

Microsoft designs and manages the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, , SOC-1, SOC-2 and FedRAMP. They also meet country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

For a full list of compliance standards that Azure adheres to, see the Compliance offerings on https://azure.micosoft.com.

9. Hosted Infrastructure Availability

Azure provides robust availability, based on extensive redundancy achieved with virtualisation technology. Azure provides numerous levels of redundancy to provide maximum availability of customers' data.

Uninterruptible power supplies and vast banks of batteries ensure that electricity remains continuous if a short-term power disruption occurs. Emergency generators provide backup power for extended outages and planned maintenance. If a natural disaster occurs, the datacentre can use onsite fuel reserves.

High-speed and robust fibre optic networks connect datacentres with other major hubs and internet users. Compute nodes host workloads closer to users to reduce latency, provide geo-redundancy, and increase overall service resiliency. A team of engineers works around the clock to ensure services are persistently available.

Microsoft ensures high availability through advanced monitoring and incident response, service support, and backup failover capability. Geographically distributed Microsoft operations centres operate 24/7/365. The Azure network is one of the largest in the world. The fibre optic and content distribution network connects datacentres and edge nodes to ensure high performance and reliability.

9.1 Disaster Recovery

Azure keeps data durable in two locations. We use the UK-South datacentre as our primary location and UK-West as the location of the backup site. In both locations, Azure constantly maintains three healthy replicas of our data.

9.2 Service Availability

Tax Systems' services are delivered using Microsoft's highly available Platform as a Service (PaaS) offering that guarantees that our service components are running, at least 99.9% of the time, without worrying about maintenance and downtimes. To provide further resilience we use geo-replication within the UK and back data up to both our data centres.

Service SLA's are provided within the appropriate service addendum.

10. Hosted Infrastructure Monitoring

10.1 Configuration and Change Management

Azure reviews and updates configuration settings and baseline configurations of hardware, software, and network devices annually. Changes are developed, tested, and approved prior to entering the production environment from a development and/or test environment.

Production environments for all Tax Systems' applications are separated from the development, testing and pre-production environments. A software versioning and revision control system is used to maintain current and historical versions of source code.

All code changes are peer-reviewed before being committed to the code-base.

Developers cannot access any production environments.

10.2 Vulnerability Management

Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure is also able to draw on the resources of the Microsoft Security Response Centre (MSRC). The MSRC identifies, monitors, responds to, and resolves security incidents and cloud vulnerabilities around the clock, every day of the year.

Tax Systems' software development security standards cover each stage of the software development lifecycle, which includes security requirement definitions, threat modelling, best practice coding standards and testing.

All code changes are peer-reviewed before being committed to the code-base; additionally, static code analysis is performed which includes reporting on security issues from the SANs Top 25 and OWASP Top 10.

10.3 Vulnerability Scanning

Vulnerability scanning is performed on server operating systems, databases, and network devices. The vulnerability scans are performed on a quarterly basis as a minimum. Azure contracts with independent assessors to perform penetration testing of the Azure boundary. Red-team exercises are also routinely performed and the results are used to make security improvements.

In addition to our in-house testing, Tax Systems engages with a third party to run penetration tests on our internal and hosted services. The last penetration test was completed by BSI in July 2019.

10.4 Protective Monitoring

Azure security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include the Microsoft Monitoring Agent (MMA) and System Centre Operations Manager. These tools are configured to provide timely alerts to Azure security personnel in situations that require immediate action.

Tax Systems uses Azure Security Centre and Azure Application Insights to monitor the security posture, compliance and availability of our systems hosted within Microsoft's Azure infrastructure. These logs feed into Microsoft Azure Sentinel, the security information event management (SIEM) and security orchestration automated response (SOAR) solution.

We have an in-house team of Engineers that use these tools to monitor and maintain our applications and infrastructure.

10.5 Incident Management

Microsoft implements a security incident management process to facilitate a coordinated response to incidents, should one occur.

If Microsoft becomes aware of unauthorised access to customer data that is stored on its equipment or in its facilities, or becomes aware of unauthorised access to such equipment or facilities resulting in loss, disclosure, or alteration of customer data, they take swift and appropriate action.

At Tax Systems, we have implemented our own incident and breach management processes to ensure we are able to provide a swift and coordinated response, should an incident or breach occur. Tax Systems will report any such incident to the data controller, without undue delay.

11. Product – MTD Compliance Portal

11.1 Product Overview

Our MTD Compliance Portal is currently made up of two products, AlphaBridge and AlphaVAT.

MTD Compliance Portal

Our cloud based MTD Compliance Portal is where you:

- Set up and manage your users and VAT entities
- Configure Role based access control
- Authorise AlphaVAT to interact with the business tax account
  n.b. AlphaBridge is the trade mark for the standalone AlphaVAT submission module, it is AlphaVAT that is authorised with HMRC
- View and manage entities with a warning system for deadlines
- View entity data as returned via the HMRC APIs in respect of obligations, payments and liabilities
- View previously submitted MTD returns
- May choose to store summary data and other digital VAT records
- Review, validate and submit the return via HMRCs API

AlphaBridge

AlphaBridge is built on top of the MTD Compliance Portal and includes the Excel template that is downloaded from the portal and is where you:

- Link in your current calculation spreadsheets to the nine box VAT Return summary in the template
- Securely post the data from the Excel template over an encrypted (HTTPS) link to our AlphaBridge API

or

- Optionally upload your existing Excel spreadsheet where the nine-box return data can be extracted from named-cells. The uploaded excel sheet is not retained on the portal.

AlphaVAT

AlphaVAT includes all of the functionality in the MTD Compliance Portal and AlphaBridge but additionally includes:

- Data management – Upload your CSV data to prepare, manage, review and check it for accuracy
- VAT Calculation & Compliance - Carry out your calculation to determine your VAT return

11.2 Product Help

For further information on product features and functionality see the support documentation here: https://webhelp.cloud.taxsystems.com/alphavat/

11.3 Application Security

The MTD Compliance Portal is securely hosted using Microsoft Azure Platform as a Service (PaaS). AlphaBridge and our APIs are protected with a Layer 7 Web Application Firewall (WAF) limiting access to HTTPS only.

Access to the portal benefits from Microsoft Azure's two-factor authentication.

AlphaBridge includes an Excel template which contains a macro to take the data from the Excel worksheet and send it over an encrypted (HTTPS) link to our API. Each Excel sheet contains its own unique cryptographic key with the API authenticating each request using HMAC authentication (HMAC-SHA256).

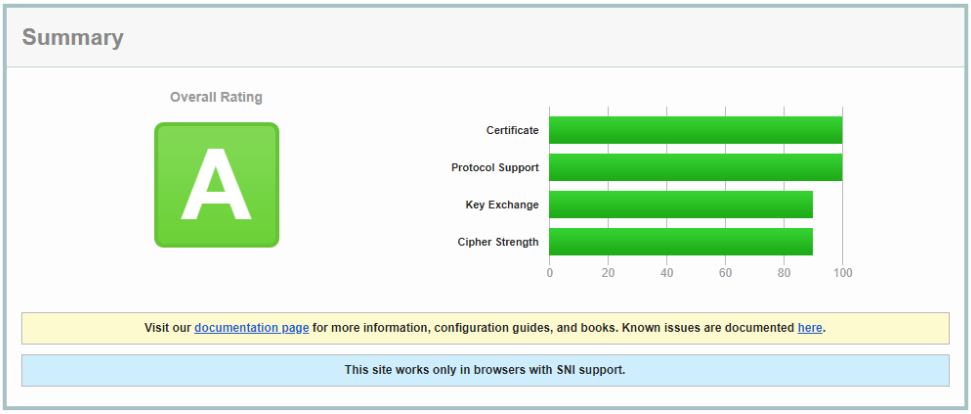
11.4 Data in Transit

All products in the MTD Compliance Portal utilise SSL / TLS Transport Layer Security (TLS) cryptographic protocols to provide end to end communications security.

Only TLS 1.2+ is supported.

We use a 2048-bit encryption key with the signature algorithm being SHA256 with RSA to secure communication between client browsers, administrative tools, and the back-end infrastructure.

Industry leader Qualys reports the servers as obtaining an "A".



11.5 Data at Rest

All data and application settings are encrypted at rest, and are done so natively.

11.6 Credential Security

User access is provided using Azure Active Directory B2C, the highly secure cloud identity platform that handles billions of authentications per day. Users can use their own company's email addresses with multifactor authentication (MFA) enforced through policy.

On setup, users are sent an email with an initial password; this password must be changed on first login. At this point the user must also provide a phone number which is then used to send a one-time code or phone call to verify possession for the "second authentication factor".

Passwords can only be reset using the Azure Active Directory service; the user must prove access to their email address and phone number in order to reset their password.

No passwords are stored within the application itself.

Administrative and infrastructure access are restricted to authorised employees. Infrastructure access is protected with an additional layer of security; requiring a service principle with a base64 encoded secure string that is only unlockable with a private key.

11.7 Application Hardening

As part of our secure software development lifecycle we use static code analysis tools to continually check our source code for security issues, bugs and vulnerabilities. Any issues are tracked and resolved through the development lifecycle.

Session Hijacking and Session Replay Attacks

Company and employee information is not stored in user cookies or session stores. We use Azure AD B2C to authenticate the user; therein OpenID Connect is used to securely sign the user into our application.

Cross-Site Request Forgery (CSRF) Attacks

To protect against forged requests, we introduce a required security token that our site knows but other sites don't know. We include the security token in requests and verify it on the server. In addition, the application adheres to the Restful request model where possible. We also include an unobtrusive scripting adapter, which adds a header called X-CSRF-Token with the security token on every request.

Injection Attacks

SQL injection attacks aim at influencing database queries by manipulating web application parameters. A popular goal of SQL injection attacks is to bypass authorization. Another goal is to carry out data manipulation or reading arbitrary data. To prevent this, Tax Systems developers adhere to the following principles.

- Avoid using client side form data directly in SQL statements server-side
- Sanitise all user input to prevent injection of invalid data or executable code
- Scope all executed code to the specific user to prevent privilege escalation

Cross-site scripting (XSS) attacks

XSS attacks are the most widespread, and one of the most devastating security vulnerabilities in web applications is XSS. This malicious attack injects client-side executable code. There are two key principles to fend of XSS attacks – Whitelists Input filtering and output escaping, both of which are principles followed by the Tax Systems development team.

Other Forms of Attack and Conclusion

In addition to the common attack mechanisms described above, other less common mechanisms, must be recognised and defended against. Tax Systems developers consider header injection, command line injection, unsafe query generation, and many other forms of attack. It is not the intent of this document to outline in details our approach to security, or indeed to provide a hacker's manual. If you have further specific questions regarding application security please do get in touch.

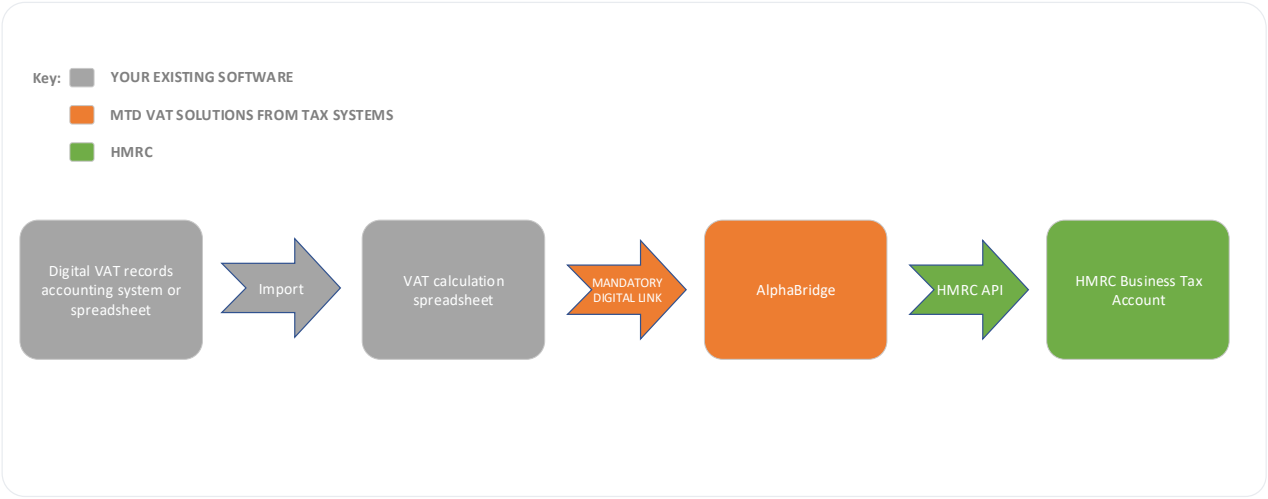
11.8 Firewalls

The MTD Compliance Portal is protected by a Web Application Firewall (WAF) that provides centralised protection of our web applications from common exploits and vulnerabilities. The WAF is automatically updated to include protection against new vulnerabilities, with no additional configuration needed.

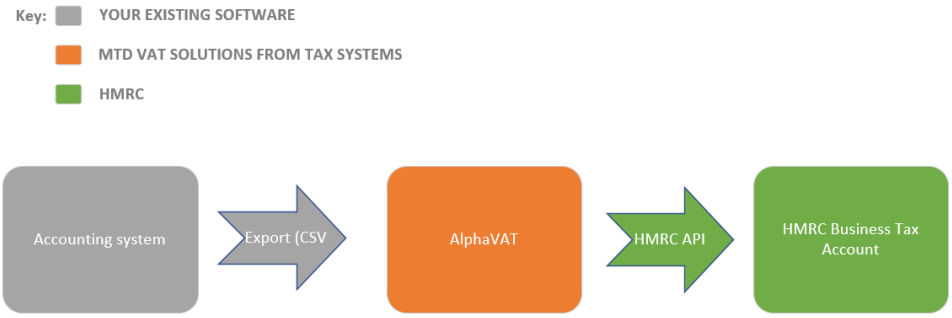
We monitor the health of our WAF and the applications that it protects with logging and integration with Azure Security Centre and Azure Sentinel SIEM.

11.9 Data Flow Diagrams

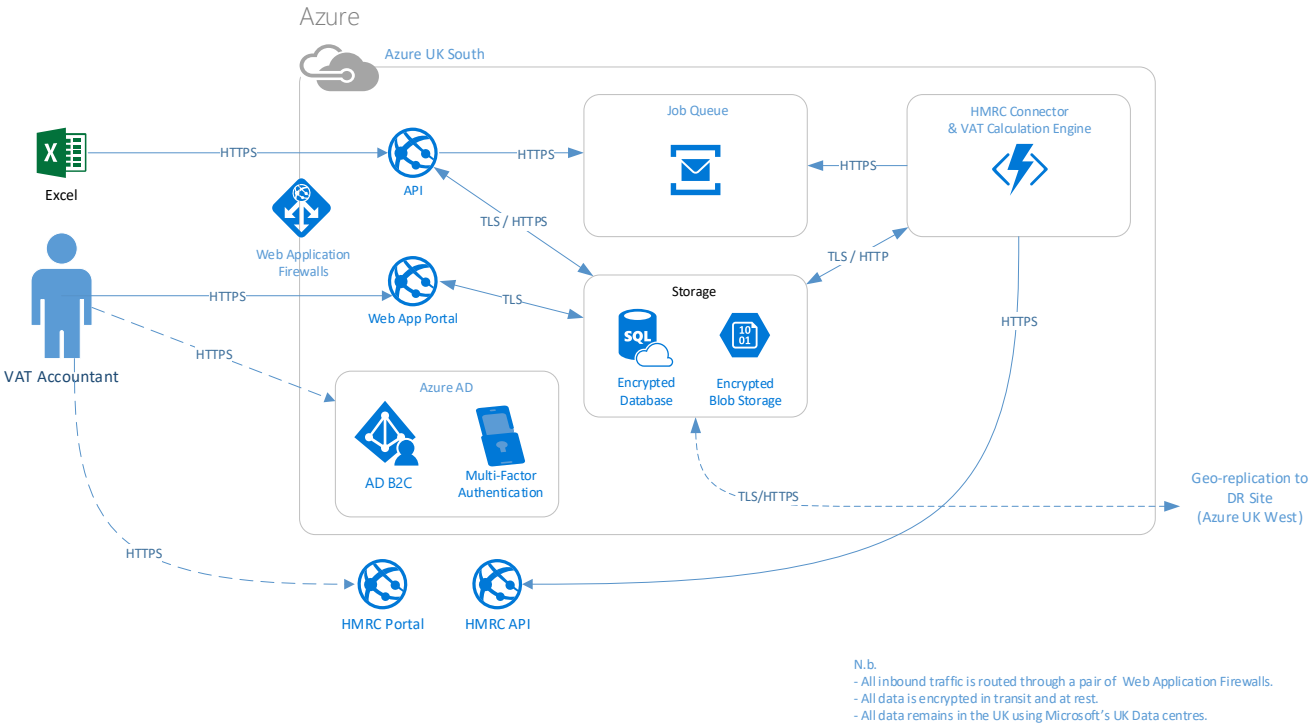
AlphaBridge



AlphaVAT



11.10 Infrastructure Diagram



11.11 Authentication

- The Excel to AlphaBridge API connection is a secure encrypted HTTPS connection authenticated with a HMAC-SHA256 token generated with a unique key per-Excel template.
- Each user of the MTD Compliance Portal is authenticated to Azure Active Directory using its multi-factor authentication service. The factors are firstly a password and secondly, a one-time code sent via SMS / or voice call.
- The MTD Compliance Portal uses OpenID Connect integrated with Azure AD to authenticate the user.
- The user must initially authorise the MTD Compliance Portal to access the HMRC API; they must login to HMRC with HMRCs multi-factor authentication before Authorising the portal.
  This supplies the portal with an OAUTH token that is then used for authentication in subsequent API requests to HMRC. This authorisation is valid for 18 months unless revoked sooner by the customer using HMRCs portal.
- All API requests to HMRC are made over a secure encrypted HTTPS connection using the OAUTH token for authentication.

The MTD Compliance portal does not currently support Single Sign On, e.g. using SAML or OpenID Connect, however should this be of interest please contact your account manager.

11.12 User Management and Roles

The MTD Compliance portal includes six different roles which a user can be assigned to that determines their level of access and what they can do within the portal.

Tax Systems will create the initial customer Superuser; the customer is then responsible for using the portal to manage user and their roles.

The roles available are:

- **Superuser:** This role has access to all User Management and Entity Management tasks and allows the user to prepare and submit VAT Returns.
- **System Admin:** This role has access to all User Management tasks, along with the Folder Option tasks within Entity Management. This allows the user to create, edit and delete other users of the portal, as well as being able to add, edit and delete folders and assign user access to folders.
- **Edit and Submit:** This role has access to all Entity Option tasks within Entity Management and allows the user to prepare and submit VAT Returns.
- **Edit:** This role has access to all Entity Option tasks within Entity Management and allows the user to prepare VAT Returns.
- **Submit only:** This role has access to view an entity's VAT return summary details and submit the VAT Return.
- **Read only:** This role has access to view an entity's VAT return summary.

Roles can only be assigned by Superusers and System Administrators.

11.13 Logging and Auditing

Azure provides a wide array of auditing and logging options to help us improve application performance and security. We collect security information from our Azure resources, the network, and connected solutions; correlating information from multiple sources with Azure Sentinel to identify threats.

The MTD Compliance portal logs all events to an internal audit log which is timestamped and cannot be altered; these logs are currently only available to Tax Systems staff but specific data can be made available via our support team on a case by case basis.

11.14 Backups

Tax Systems utilise Microsoft Azure's standard backup and geo-replication facilities.

The AlphaVAT service provides the following service levels.

- Recovery Point Objective (RPO): < One hour.
- Recover Time Objective (RTO): < Six hours during Core Business Hours.

The following provides further technical details on the backup services that we utilise.

SQL Databases:

- Point-in-time Restore over the last 35 days.
  This is achieved by
    - Full database backups are created weekly, differential database backups are created every 12 hours, and transaction log backups are created every 5 - 10 minutes, with the frequency based on the compute size and amount of database activity.
    - Backups are geo-replicated offsite to the secondary UK datacentre.
- Long Term backups
    - These are stored - Weekly for 3 months; Monthly for 15 months; Yearly for 7 years.
    - Backups are geo-replicated offsite to the secondary UK datacentre.
- All back-ups are encrypted at rest.
- Databases also use active geo-replication to create readable replicas at the secondary UK datacentre. There is a manual process to failover to these replicas and make them writeable.

Azure Storage Accounts (Blob storage):

- Data is Geo-replicated to the secondary UK Data centre using Geo-redundant storage.
- Geo-redundant storage is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year by replicating data to a secondary region that is hundreds of miles away from the primary region (but still within the UK).
- All data is first replicated with locally redundant storage (LRS). An update is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region using GRS. When data is written to the secondary location, it's also replicated within that location using LRS.
- Azure Storage encryption is used to encrypt all data at rest.
- All files stored with Azure Storage utilise "Soft-deletion" where by if they are deleted or overwritten a snapshot is taken and is available for 365 days should it need to be recovered.

12. Product Support

Tax Systems' innovative automation technology and compliance services helps corporations and advisors make their processes more efficient, reducing operational risk and enabling expert professionals to focus on delivering more value to their business or clients.

We focus considerable resources on providing comprehensive training and support to our customers so they realise the full potential of our software. Our training and support services are highly regarded by our customers; achieving high levels of customer satisfaction and resolving more than 60% of calls at the first point of contact.

12.1 Contacting Support

We offer two forms of support to our customers; manned telephone support and monitored email support.

- Telephone support: 9:00 A.M. to 5:30 P.M. Monday – Friday, excluding English public holidays
- Calls received out of office hours will be forwarded to voicemail and action will be taken the next working day
- Email support: Monitored 9:00 A.M. to 5:30 P.M. Monday – Friday, excluding English public holidays
- Emails received outside of office hours will be collected and action will be taken the next working day

12.2 Support Overview

- Over half of support queries that are received through our support lines are answered and closed at the initial contact.
- Calls that require further investigation or analysis are passed to our second level support who will liaise with the customer.
- Third Line and engineering can draw upon additional resource from tax experts, systems or business professionals as required.

12.3 Case categorisation

All cases pass through categorisation and prioritisation – these form the basis on which the SLA's are provided. It is important that the customer provides all of the necessary information relating to the case as soon as possible, so that a resolution can be sought.

This includes, but is not limited to:

- Infrastructure specifications
- Files required to replicate the issue
- Detailed steps to reproduce issue
- Relevant tax legislation, where tax interpretation is queried.

Cases are categorised between **Service requests**, **Incidents** and **Enhancements** as defined by ITIL.

Service requests are defined as a formal request from a user for something to be provided – for example, a request for information or advice. For example, a user wants to know how a particular statement or set of tax rules are operating within Alphatax.

Incident cases are defined as unplanned interruptions. For example, the user cannot submit their tax return due to a software issue.

Enhancement requests (or feature requests) are defined as additional features which are deemed useful with potential time-saving or product usability benefits in a particular use case.

12.4 Case Prioritisation

Incident and **service request** cases are prioritised between 1 and 5 and are calculated using a combination of Urgency and Impact. Examples of how these are defined are below.

Enhancement cases do not pass through the case prioritisation routine. These are instead added to a backlog along with other feature requests and prioritised in future releases based on customer demand.

12.5 Support Staff Training

On-going internal training is provided to ensure support staff have expert knowledge of our products, new product features, processes and changes to legislative and regulatory requirements.

12.6 Support Data

If customer data is required to troubleshoot an issue, it will be requested that this is sent securely, encrypted and password protected. The data will be stored on an encrypted disk that is excluded from backups and will be deleted once the support request is resolved.

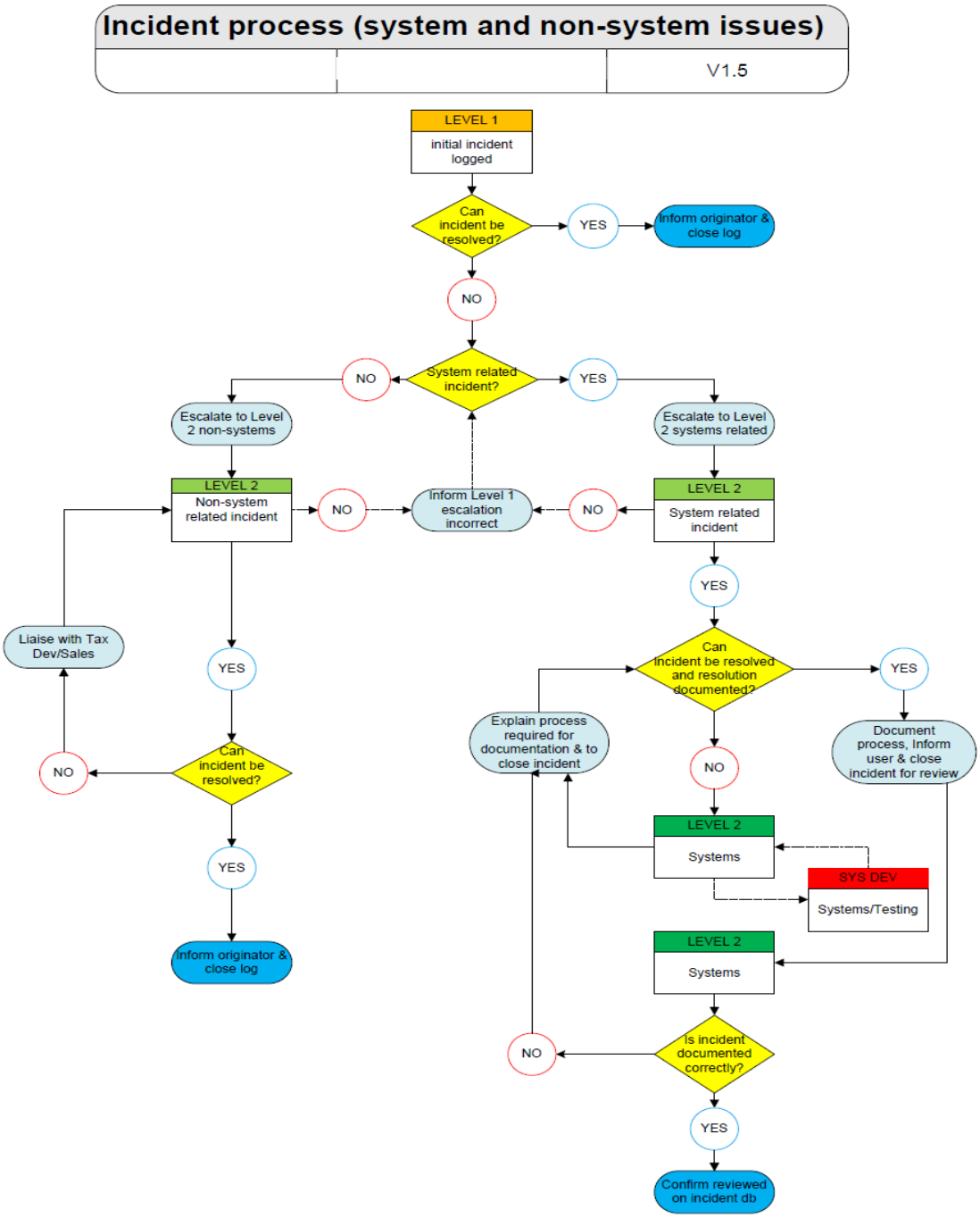
12.7 Incident Review

Tax Systems prides itself on providing exceptional support to our customers, but we are always looking at ways to make it even better.

One of the ways we achieve continuous improvement is to conduct a post-incident review of each incident, capturing the root cause and other relevant information. This information is collated and reviewed by a cross-departmental group and reported to management.

Root cause information of any incident can be requested from your support representative.

12.8 Incident Response Process



Tax Computer Systems Limited
Magna House, 18 – 32 London Road,
Staines-Upon-Thames, TW18 4BP
T: 01784 777 700
E: enquiries@taxsystems.com
W: www.taxsystems.com