Prism Information Security Pack

DATE: 07-May-2025 v1.0

Connecting people to work

Purpose

To assist clients with completing a security review of our Prism platform we have brought together an overview of our Technical and Operational controls in place which are designed to safeguard the services we provide and the data which we process. Further information on technical & security configurations, dataflows, policies, and procedures are available upon request.

This platform provides clients of Team Matrix (Matrix SCM Ltd and Sec Watchdog Ltd) functionality for the procurement and management of permanent and contingency workers, statement of works, pre-employment screening and associated data reporting and analytics.

Organisation

Team Matrix consists of two Limited companies that are consolidated into a further Group ownership structure that is related to our Private Equity investor requirements, the two companies and associated services are as follows:

- Sec Watchdog Limited – Company Registration Number: 14616198

Security Watchdog performs pre-employment screening services including digital identification verification, right-to-work, criminality, and social media checks to organisations largely across the UK, but also in conjunction with partners to non-UK companies, or non-UK entities of UK based companies..

Customers include the likes of British Aerospace, Financial Conduct Authority, Vodaphone and a number of banks and other financial institutions through to small businesses, charities, or even small volunteering groups (such as kids sports clubs) that require volunteers to have Disclosure and Barring Service checks.

- Matrix SCM Limited – Company Registration Number: 02227962

Matrix SCM provides platform and services related to the recruitment and management of both contingent and permanent workers. It also provides a statement-of-works platform and service too.

This service sits between a supply chain of 2000+ recruitment agencies in the UK and large (by employee count) employers.

Many of these employers are public sector, local authorities, but also include private sector businesses such as a large supermarket chain with ~700 sites and multiple care home providers. The platform and service facilitate the recruitment and management of contingent workers and also permanent recruitment.

As above both Sec Watchdog Limited and Matrix SCM Limited are subsidiaries of Azure; Company Registration Number: which is owned by Bridgepoint PLC; Company Registration Number 11443992

The registered address for both Matrix SCM Ltd and Sec Watchdog Limited is as follows, this is also the location where the supplied services are managed:

Partis House
5 Davy Avenue
Milton Keynes
MK5 8HJ

Are we a Regulated Entity

Neither Sec Watchdog Limited nor Matrix SCM Limited are regulated entities, though we do have professional memberships with for following:

- PBSA (Professional Background Screening Organisation)
- FCSA (Freelancer & Contractor Services Association) accredited

Certifications and Accreditations

At Team Matrix we ensure that our information and data security, quality management and environmental responsibilities are second to none, as such we hold the following suite of internationally recognised and independently audited accreditations and certificates. Our ongoing compliance with these standards is audited through UKAS & IASME approved certification bodies on a yearly basis to ensure we meet the stringent standard required.

- **ISO 27001:2022** Information Security, Cybersecurity and Privacy Protection
  - The globally recognized gold standard for the implementation and ongoing management of an Information Security Management System (ISMS).
  - Across Team Matrix this accreditation has been held for 9 years.

- **ISO 9001**: **2015** Quality Management Systems (QMS)
  - Adherence to this accreditation ensures that we provide constantly high-quality services and outcomes to our clients.
  - Across Team Matrix this accreditation has been held for 8 years.

- **ISO 14001: 2015** Environmental Management System (EMS).
  - Implementation of this accreditation has enabled us to minimise our current environmental impact and introduce measures which will reduce our impact even further in the future.
  - Across Team Matrix this accreditation has been held for 4 years.

- **Cyber Essentials Plus**
  - This UK government backed, IASME managed accreditation ensures adherence to UK industry best practices regarding technical security and vulnerability management.
  - Across Team Matrix this certification has been held for 4 years.

Copies of our certificates are available upon request.

ICO Registration Details

Matrix SCM Limited: Z1146191

Sec Watchdog Limited: ZB557376

Key Security, Data Protection and Risk Contacts

- Barry Gallivan – Information Security Manager
- Scott Ashenden – Head of Infrastructure and Security
- Lauren Edwards – Data Protection Officer
- Ashley Doody – Chief Product and Technology Officer
- Rob Allinson – Chief Risk and Business Assurance Officer

Introduction to Prism

Matrix Prism is a Workforce management solution. It is cloud based and is hosted in a fully managed AWS environment. It is developed using an enterprise grade Low-Code development tool from OutSystems, who are a leading provider and visionary in this field on the Gartner Quadrant.

1. Data Encryption

Data is sent securely from the end-user device over a HTTPS/TLS connection that is encrypted through an SSL certificate obtained from a trusted certificate authority, we utilise TLS 1.2 as standard with TLS 1.3 configured where system capability allows, always using secure ciphers. This ensures all data in transit is fully secured, it cannot be intercepted or tampered with during transmission.

- Data in transit is protected internally within the service.
    - The service operates in a fully hosted environment in AWS.
    - Data is encrypted in transit using TLS 1.2 or TLS 1.3
- Data in transit is protected between the service and other services (e.g. where APIs are exposed).
    - Any data transferred between Matrix and other services is strictly controlled through authentication methods and is sent securely using HTTPS connection to a Web API.
    - For larger transfers where API is not appropriate, SFTP is used.
- Data at rest is encrypted.
    - Data is stored at rest in a SQL Server database in the internal part of the network encrypted to AES-256
    - Backups are stored in a separate data centre and are also encrypted at using AES-256.
    - End user devices have full disk encryption in place.

2. Asset Management, Protection and Resilience

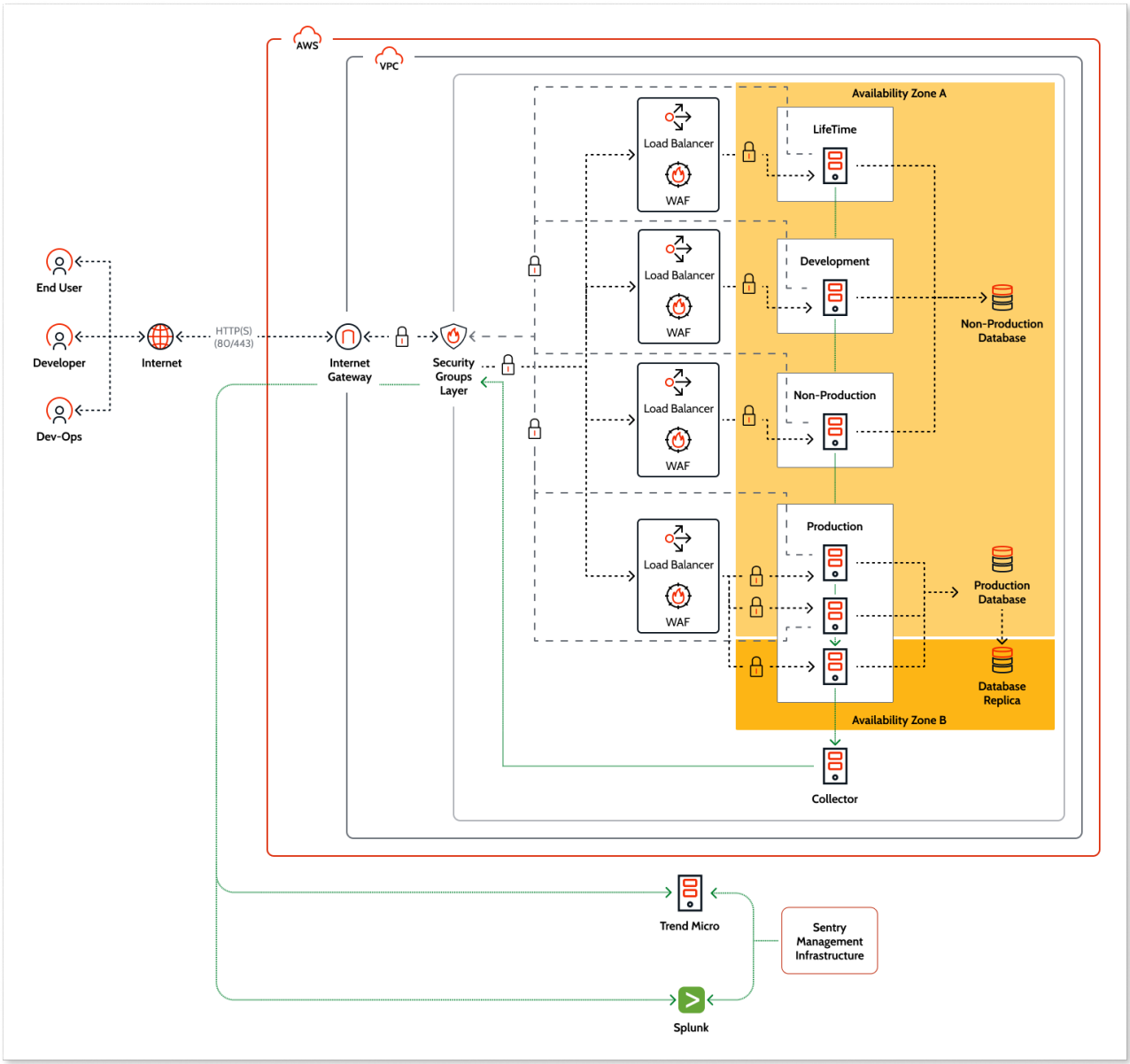
All Matrix personnel are provided with a security hardened laptop fully managed by our IT teams; we adhere to the standards defined in the CIS framework to ensure comprehensive device security and maintain a comprehensive register of all our assets.

All devices are monitored for security compliance, we have automatic updates in place across our estate, including automated patch deployment, application, and OS update management in place. Any devices which do are not in compliance are investigated and compliance is manually achieved by out IT staff.

Prism is hosted in AWS on a dedicated virtualized environment that is protected by a virtual private cloud, logically isolated from the internet and other networks in the AWS cloud. This environment is fully managed by the OutSystems infrastructure team, with dedicated support from AWS. Matrix do not have

any direct connection to the servers themselves. Limited changes can be requested through a support process.

Separate environments are configured for development, test UAT and production in separate virtualised environments and the environment is configured to operate in High-Availability mode. Please see below for a High-Level Diagram of the AWS environment.



3. Separation between users

Prism is a multi-tenancy designed solution whereby all users log into the same site to access their data, meaning strict access controls are imperative the security of the data within. Client separation is

enforced logically in the database layer, using a table-based multitenancy design to provide isolation through a tenant identifier column.

Client separation is also enforced in the presentation layer by implementing a robust security mechanism that provides the extra logic to make sure that each customer is only allowed to see its own data and prevent any leakage.

We adhere to the principle of least privilege and enforce Role Base Access Controls (RBAC) across all of our estate, systems, and applications, this ensures only those who need to see specific data, can do so.

Access to the system is granted to authorised users only, each client installation will manage their own user base, and each user must have their own account, and user roles define what access the user has to data and the actions they can perform.

All users have unique credentials to login and all activity is recorded and changes audited.

4. Operational security

We have in place a range of technical and operational security measures to ensure the Confidentiality, Integrity, and Availability of data we handle, overall governance is provided by our Information Security Management System (ISMS) with technical controls implemented according to industry best practices.

Prism is hosted in a secure and dedicated virtualised environment in AWS; this is fully managed and supported by OutSystems infrastructure support team and has been designed with security at the forefront of all operations with a dedicated SecOps team to support.

A range of technical controls are in place including Web Application Firewalls, Intrusion Detection & Intrusion Prevention Systems, URL blocklisting, USB block, Vulnerability Scanning, Anti-Virus & Anti-Malware and appropriate user and security logging, monitoring, and alerting across the system.

All Matrix devices are centrally managed in our MDM solution and security hardened following the CIS guidelines and are automatically monitored for compliance, this MDM solution also provides remote access to all end user devices, including a remote wipe functionality.

All user accounts are centrally managed adhering to the principle of least privilege, Role Base Access Controls (RBAC) is in place across our estate, all accounts number matching MFA enforced.

Security groups are used to control user access and are regularly audited. Selected IT personnel have a separate Admin account which are monitored and used only for the purpose of administrative activities.

The environment is also configured to provide High availability with near instant failover to a secondary environment in the event of a BC/DR event occurs, this is supported by regular backups of all virtual machines and databased. BC/DR testing is conducted to ensure any failover or recovery of data will be successful should it be needed.

Patching is carried out in line with industry best practices, regular vulnerability scans are conducted, and any identified vulnerabilities are assessed and remediated accordingly.

Annual penetration tests are arranged by Team Matrix using independent third parties, managed by our Information Security Manager, testing is conducted in line with industry best practices and our vulnerability management policies and processes.

Physical security controls are in place across our offices, this include CCTV through-out our offices, access cards are on office entry and also on secure areas, which are also limited to key personnel only, visitor processes are in place and training is provided to all staff on office security and visitor processes.

Access to the AWS cloud data centred is managed by AWS, details of the controls in place can be found on their website Data Centers - Our Controls

Public access to the Prism application is controlled through security authentication methods, all users must login before being able to access to the features.

The Prism platform employs a multi-layered security approach to protect applications and data, including network security, secure application code, and data protection measures. Key features include intrusion detection, AWS Shield for DDoS protection, and Sentry for enterprise-grade security.

Administration of Prism in managed through 2 OutSystems portals – Service Centre and Lifetime. This is where the different environments are defined, applications configured and infrastructure customised. The development teams and roles are also configured in this portal and only IT personnel with certain administrative authority can access these portals and all actions are audited.

5. HR security

We ensure that all staff are vetted and trained before they have access to any of our sensitive systems or any client data, compliance to screening requirements and training is managed by our HR team.

Our joiner, movers and leavers process is managed by our HR and IT teams, this ensures that all staff (new or moving) are assigned access only based on their individual role and we have full traceability of all approvals, assignments, and actions. This process also ensures that when staff leave the company their access is revoked at the end of their last day (and always within 24 hours) and that all equipment is returned.

5.1 Background checks

All staff undergo pre-employment screening checks before starting with us, as a minimum these include (but are not limited to) the following:

- 3-year Financial Probity.
- Right to Work and ID check.
- International Sanctions and PEP check.
- Media Check.
- 3-year referencing checks.
- Criminality Check.

For more senior or critical roles, the following checks can be conducted:

- BPSS, Security Check
- Developed Vetting
- Any international or national terror or watch list checks

5.2 Security training

All Matrix personnel undergo Information Security and Data Protection Training during their induction delivered by our Information Security Manager and Data Protection Officer; this training is complemented by our online training modules and is regularly updated.

Attendance and training completion are monitored and actioned appropriately, all training is re-issued on an annual basis and ad-hoc training is provided on new and emerging threats as required.

Regular phishing simulations are conducted throughout the year, with simulations based on the latest threat intel and identified threats which our business faces.

All staff are required to read and acknowledge all applicable Information Security and Data Protection policies which are available companywide via our HR system.

6. Secure Development

The Prism system within OutSystems is designed to ensure that robust security measures are seamlessly integrated into every phase of the development lifecycle, they have a comprehensive Secure Development Lifecycle (SDLC) which includes risk assessing every change before it is approved, are a member of the Cloud Security Alliance (CSA) and Centre for Internet Security (CIS), demonstrating their commitment to secure cloud application development.

Code is developed using the Designer Studio against a development database, a range of automated security assessments check the quality of code as well as identifying vulnerabilities before the release cycle, code reviews are carried out at all stages of development, and there are fully segregated test, pre-production, and production environments.

To ensure the above control work as expected, prior to any significant piece of development work being released Team Matrix engage an independent third party to conduct penetration testing, with any findings being remediated before go-live.

7. Supply chain security

Supply chain security is key to ensuring all the data we handle, and process is stored and processed securely, in line with our policies, procedures, and all applicable laws and regulations.

To ensure this, all suppliers within our supply chain to are audited and risk assessed by our Information Security Manager and Data Protection Officer before they are onboarded, and all suppliers undergo annual information security and data protection due diligence risk assessments to ensure continued compliance to our security standards.

The Matrix Workforce division heavily utilises a supply chain of recruitment agencies to provide our services, these agencies undergo additional checks including credit checks and we also hold copies of insurance certificates and indemnity policies, as well as signing a supplier agreement which has provisions for data protection and information security requirements.

8. Secure user management

User Management in Matrix Prism builds on top of OutSystems' comprehensive and secure user management principles. In transit and at rest, user and authentication-related information is SHA-256 encrypted.

Once onboarded, every customer is allocated a unique system-wide identifier that is replicated against their users. Customers can allocate role-based access to the specific product areas & features they would like their users to interact with; the customer administrators have access to a User Management application which allows them to be in full control of the user records and on/off boarding processes.

For security and compliance purposes, our system monitors and logs all interactions with user records and their respective login, session and activity history in our system and this data is available to the customer administrators only.

9. Identity and Authentication

Every user has their own login to the system, with authentication is provided through a unique username and password with two factor authentication available to be configured, whereby a code is emailed to the registered email address that the user then must enter a second authentication page.

Single sign-on is also supported using any SAML provider - ADFS, Azure, Google, and works in conjunction with MFA to provide greater account security.

The system enforces the use of strong passwords that must be changed regularly. Accounts are automatically locked out after 7 failed attempts. Additional security and brute force protections are in place, including shorter failed login attempts and Captcha, and all login activity is recorded.

All passwords are encrypted at rest and in transit and stored using one-way encryption in the database.

10. Secure service administration

Administration of Prism in managed through two OutSystems portals – Service Centre and Lifetime. This is where the different environments are defined, applications configured and infrastructure customised. The development teams and roles are also configured in this portal and only IT personnel with certain administrative authority can access these portals and all actions are audited.

11. Audit information for user

At the application level, user activity is audited through the code. Data changes are timestamped, and audit trails are kept. These show the lifetime of each entity, from creation through to completion and what changes are made.

The main OutSystems infrastructure portal is only accessible by the Matrix IT admin team. This is where the different environments are defined, applications configured and infrastructure customised. This is also where the development teams and roles are configured.

OutSystems automatically logs every task performed by the IT admin users to ensure there is full traceability of the entire deployment, and these audit logs are kept for 365 days

Other information is recorded such as application errors, screen requests, service actions, API requests and excessive login attempts are logged and kept for rolling 7 days.

12. Secure use of the service

Matrix Prism is a publicly accessible cloud service that can only be accessed by registered users, and there are three types of User persona:

- Customers looking to fill roles,
- Recruitment agencies sourcing suitable candidates, and
- Matrix employees providing back-office support roles.

Customers have a contracted agreement with Matrix to use the application, and the managers are onboarded by our implementation team.

Recruitment agencies looking to join the Matrix supply chain have to enrol first and are fully vetted before being allowed to use the system. Their agents can self-register

The Matrix employees who have access to the system are fully trained on how to use the service

Every user is required to login to access the service with their unique ID, user roles control the access to what data each user is allowed to see and, also what actions they can perform.

Audit Logs track specific user activity including login/logout, pages visited and the data that they change.