XGRC® SOFTWARE by Strategix

SECURITY & TRUST OVERVIEW

How we protect the records you are audited on

Security, privacy and resilience of the XGRC® platform: the answers procurement, security and legal teams need before they buy.

ISO/IEC 27001:2022
Certified by BSI, certificate IS 804839

Immediate
Breach notice, and within 72 hours at most

RPO 1h · RTO 4h
Recovery objectives, tested quarterly

AES-256
At rest, with per-customer keys

SYNERGY IN ASSURANCE, STRENGTH IN COMPLIANCE®

Strategix Application Solutions (Pty) Ltd · developer and operator of XGRC® Software

xgrcsoftware.com/trust

Contents

· At a glance

1 Executive summary

2 Governance and certification

3 Hosting, architecture and data residency

4 Data protection and privacy

5 Encryption and key management

6 Identity and access management

7 Application security and vulnerabilities

8 Security monitoring and operations

9 Incident response and breach notification

10 Business continuity and disaster recovery

11 Supplier, people and physical security

12 AI governance: MAIA® and AI agents

13 Support, maintenance and service levels

14 Shared responsibility and assurance

15 Privacy law: POPIA, PAIA and GDPR

16 Frequently asked security questions

A ISMS documents

B Related documents and contact

At a glance

> The facts procurement and security teams ask for first.

CERTIFICATION
ISO/IEC 27001:2022, certified by BSI (certificate IS 804839, valid to 28 August 2027), covering the design, development, delivery and support of the XGRC® cloud platform

HOSTING
Microsoft Azure, West Europe (Netherlands). Azure holds ISO 27001, ISO 27017, ISO 27018 and SOC 2 Type II

DEPLOYMENT
Cloud SaaS, multi-tenant with strict logical isolation between customers

ENCRYPTION
TLS 1.2 or higher in transit; AES-256 at rest, with keys unique to each customer

SIGN-IN
Single sign-on and MFA with Microsoft Entra ID; MFA enforced for all Strategix administrative access

ACCESS CONTROL
Role-based, down to module, dashboard and record; new modules start with no access

BREACH NOTIFICATION
Immediately once we have reasonable grounds to believe personal information was compromised, and within 72 hours of a confirmed incident

SECURITY INCIDENT RESPONSE
Severity 0: initial response within 4 hours, 24 hours a day, 7 days a week

RECOVERY
RPO 1 hour, RTO 4 hours

PRIVACY
POPIA and GDPR; Data Processing Addendum meets POPIA section 21 and GDPR Article 28

SUBPROCESSORS
Two: Microsoft Azure (hosting) and Microsoft 365 (email), both in West Europe; 10 business days' notice of material changes

YOUR DATA
Yours. Copy on request within 30 days of exit; deleted within 90 days, with a Data Destruction Certificate

1 Executive summary

> The XGRC® platform holds the records organisations are audited on: risks, incidents, controls, obligations, suppliers and evidence. We protect it accordingly, under an ISO/IEC 27001:2022 certified information security management system.

Strategix Application Solutions (Pty) Ltd is the original developer and operator of XGRC®. More than 800 companies on six continents use it. That gives us one responsibility above all others: the information you put into XGRC® stays confidential, intact and available, and remains yours.

This document explains how we meet that responsibility, from governance and hosting to encryption, access, monitoring, incident response, recovery, suppliers and AI. Where a commitment is contractual, we name the document that carries it: the XGRC® SaaS Agreement, the Data Processing Addendum, the Support Policy and the Cybersecurity & Data Protection Policy, all published in our Trust Centre at xgrcsoftware.com/trust.

We also run our own information security management system on XGRC® itself. The policies, risks, controls, vulnerabilities and audits described here are recorded, assessed and tracked in the same platform our customers use.

2 Governance and certification

> Our information security management system (ISMS) is certified to ISO/IEC 27001:2022.

Its scope covers the design, development, delivery and support of the XGRC® cloud-based platform. BSI issued the certificate, IS 804839, on 29 August 2024; it is valid until 28 August 2027, and anyone can check it in BSI's public certificate directory.

How the ISMS works

- **Policies:** a documented Information Security Policy and supporting policies for access control, cryptography, asset management, supplier security, communications, physical security, business continuity, incident management and secure development (Appendix A lists them).
- **Risk management:** information security risks are assessed and treated through a documented process, with a Statement of Applicability against the ISO/IEC 27001:2022 Annex A controls and a maintained risk treatment plan.
- **Roles:** defined roles, responsibilities and authorities for information security, with management accountable for the ISMS.
- **Measurement:** security objectives, a monitoring and measurement plan, an internal audit programme and management reviews.
- **Improvement:** nonconformities and corrective actions are logged and closed through a continual improvement process.
- **External audit:** an independent certification body audits the ISMS every year, with a full recertification audit every three years.

Frameworks we align to

Alongside ISO/IEC 27001:2022, our security practices draw on the NIST Cybersecurity Framework (identify, protect, detect, respond, recover), the CIS Critical Security Controls and the OWASP Top 10 for web application risks.

Privacy law

We operate under South Africa's Protection of Personal Information Act (POPIA) and, where it applies to our customers, the EU General Data Protection Regulation (GDPR). Section 4 explains how.

Compliance monitoring

Compliance is monitored continuously, both for our own ISMS and for the obligations our customers track in XGRC®. Regulatory content and platform controls are updated as laws and standards change, so customers stay ahead of new requirements and reduce the risk of fines and penalties.

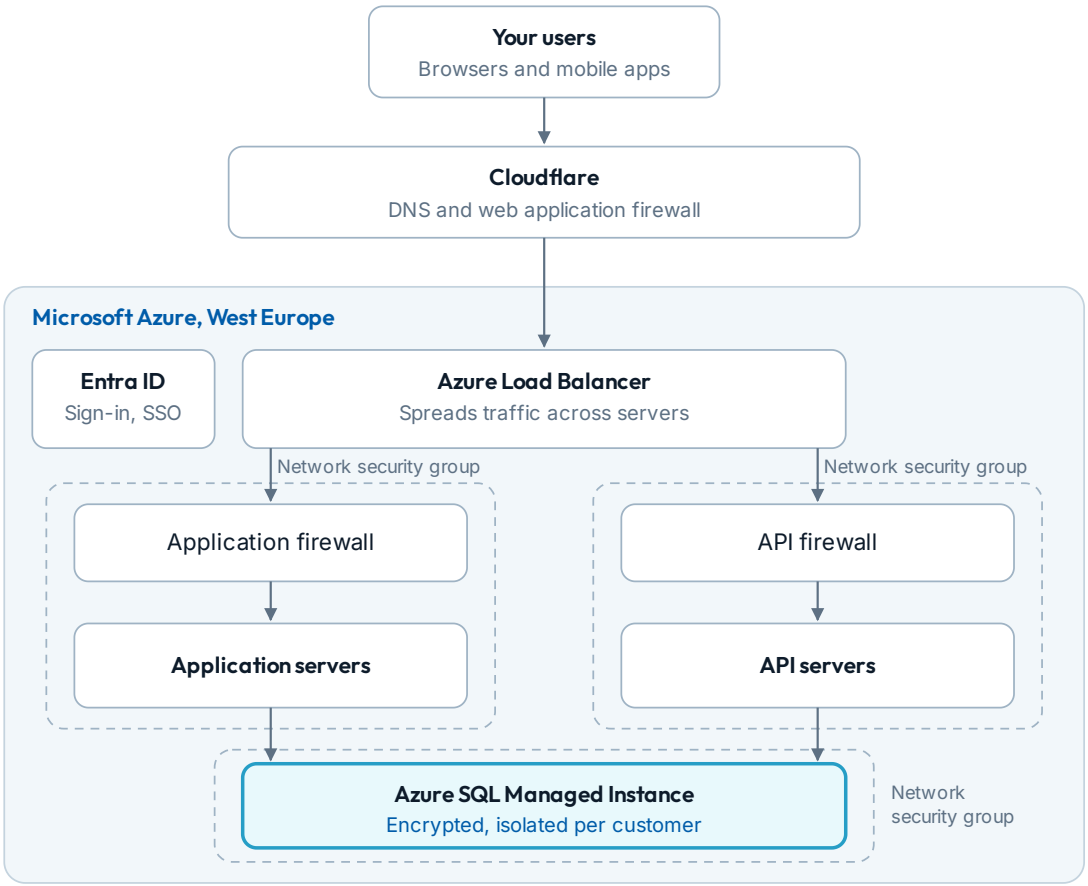
3 Hosting, architecture and data residency

> XGRC® runs on Microsoft Azure in the West Europe region (Netherlands), behind layered network defences, with every customer's data logically isolated from every other.

Where your data lives

- **Primary hosting:** Microsoft Azure, West Europe (Netherlands). Customer Data is stored there.
- **Microsoft's own assurance:** Azure's infrastructure holds ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and SOC 2 Type II certifications, and Microsoft runs the physical data centre security.
- **Subprocessors:** Microsoft Azure (hosting, infrastructure, storage) and Microsoft 365 (email delivery and notifications), both in West Europe. The live list is at xgrcsoftware.com/trust/subprocessors. Hakware, our security operations partner, sees only technical security telemetry, so it is not a subprocessor.
- **Cross-border transfers:** where personal information leaves South Africa, it is protected by the safeguards in the Data Processing Addendum and applicable law.

How the platform is built



Traffic passes five layers of defence before it reaches your data. High-level view; detailed network and infrastructure maps are not shared, to protect the platform.

- **Edge:** Cloudflare DNS and web application firewall filter traffic and block common web attacks before they reach Azure.
- **Application and API tiers:** separate application and API sets, each behind its own web application firewall.
- **Load balancing:** Azure Load Balancer spreads traffic across servers for availability.

- **Network segregation:** network security groups restrict traffic between tiers to what each needs.
- **Data tier:** Azure SQL Managed Instance, reachable only from the application tiers.
- **Identity:** Microsoft Entra ID for authentication and single sign-on.
- **Scaling:** resources scale automatically under heavy load, so peaks do not degrade service.

Multi-tenancy

XGRC® is a multi-tenant platform with strict logical data isolation between customers, so one customer cannot see another's data.

4 Data protection and privacy

> You own your data. We process it only on your documented instructions, under a Data Processing Addendum written to POPIA section 21 and GDPR Article 28.

Topic	Our commitment	Where it is written
Roles	You are the Responsible Party (controller); Strategix is the Operator (processor)	Data Processing Addendum, s3
Purpose	Personal information is processed only to provide and support the service: hosting, user management, support, backup, recovery and security monitoring	DPA, s4
No other use	Never used for any independent purpose, never sold, never disclosed except to deliver the service or where law requires	DPA, s6; Privacy Policy
Confidentiality	Everyone with access is bound by confidentiality obligations	DPA, s6
Subprocessors	Same-strength contractual terms; Strategix stays responsible; 10 business days' notice of material changes and a right to object	DPA, s8; Subprocessor List
Data subject requests	Reasonable assistance with access, correction and deletion requests	DPA, s10
Security incidents	Immediate notification once there are reasonable grounds to believe personal information was compromised (POPIA s21(2)), and within 72 hours of a confirmed incident, with nature, scope, likely consequences and remediation	DPA, s11
Return	A copy of your data on request within 30 days of termination	DPA, s12
Deletion	Personal information deleted or irreversibly anonymised within 90 days of termination; backups stay protected until overwritten. A Data Destruction Certificate is issued once deletion is complete	DPA, s12
Evidence	Certificates, audit summaries or control statements on written request	DPA, s13
Changes	30 days' notice of material changes to the DPA	DPA, s15

The DPA, Privacy Policy, Subprocessor List and Data Hosting pages are published in full in our Trust Centre.

5 Encryption and key management

> Your data is encrypted whenever it moves and wherever it is stored.

- **In transit:** all traffic between users, the platform and its services uses TLS 1.2 or TLS 1.3. Plain HTTP is redirected to HTTPS, and browsers are instructed to use HTTPS only (HTTP Strict Transport Security).
- **At rest:** stored data is encrypted with AES-256, the 256-bit Rijndael standard.
- **Per-customer keys:** each customer's data is encrypted with keys unique to that customer, so one customer's key cannot open another's data.
- **Key management:** keys are generated, stored, rotated and retired under our Cryptography Policy, with access limited to authorised personnel.
- **Mobile:** data the SHEQX® mobile apps capture offline is encrypted on the device, and users can clear it from the device at any time. The app keeps its reference data after syncing, so it keeps working offline without downloading everything again.

6 Identity and access management

> Your administrators decide exactly who sees what, down to a single record; our own staff get only the access their role needs.

For your users

- **Single sign-on:** users can sign in through Microsoft Entra ID (Azure Active Directory), so your own password, MFA and leaver policies apply. Microsoft Entra ID is the supported identity provider for SSO.
- **Multi-factor authentication:** applied to your users through Microsoft Entra ID, under your own MFA policies.
- **Granular permissions:** administrators set add, edit, view and delete rights per module, dashboard and record.
- **Record-level security:** access can be limited by business unit and category, so people see only the records that belong to them.
- **Least access by default:** newly released features and modules start with no access until your administrator grants it, so an update never widens access silently.
- **Audit trail:** changes to records are logged with who made them and when.

For Strategix staff

- Access to production systems follows least privilege and is granted per role under our Access Control Policy.
- Multi-factor authentication is required for all administrative access.
- Access is reviewed regularly and removed promptly when people change role or leave.

7 Application security, vulnerabilities and change control

> We look for weaknesses every day and close the serious ones immediately, outside the normal release cycle.

- **Secure development:** XGRC® is developed under our System Acquisition, Development and Maintenance Policy, designed against the OWASP Top 10 web application risks.
- **Change control:** every platform change follows a documented change control process.
- **Vulnerability scanning:** automated, AI-driven vulnerability assessments run daily through Hakware, our penetration-testing and vulnerability partner.
- **Tracked to closure:** each finding is recorded in XGRC® as a risk, assessed, given an action plan and closed with a control, the same way our customers manage theirs.
- **Penetration testing:** automated penetration testing runs daily, and a manual penetration test is carried out every year; an executive summary is available under NDA.
- **Patching:** critical security patches are deployed immediately, outside regular update cycles, with little or no disruption to service.
- **Browser protections:** the platform sends security headers that block clickjacking and content-type sniffing, alongside HTTPS-only enforcement.

8 Security monitoring and operations

> The platform is watched around the clock, so threats are found and contained quickly.

- **Security operations centre:** 24/7 monitoring by Hakware's security operations centre, using real-time threat intelligence.
- **SIEM:** security events from across the environment are collected and correlated in real time.
- **SOAR:** security orchestration, automation and response speeds up detection and containment.
- **Logging:** security, access and audit events are logged and retained indefinitely, so an investigation can always go back to the start.
- **Server hardening:** servers are hardened, with segregated system layers and restricted access to critical functions.
- **Capacity and performance:** resources and performance are monitored continuously, with automatic scaling under load.

9 Incident response and breach notification

> A suspected security breach gets a response within 4 hours, at any hour, and we notify you immediately once we have reasonable grounds to believe your personal information was compromised, and within 72 hours of confirming an incident.

How we respond

Our Incident Response Team works to documented procedures in the ISMS:

01
Identify
Detect the incident and determine its scope and severity.

02
Contain
Limit the impact and stop further damage.

03
Eradicate
Remove the root cause.

04
Recover
Restore affected systems to full function, with the weakness closed.

05
Learn
Review the incident and strengthen controls and procedures.

Our commitments

Commitment	Target	Source
Initial response to a confirmed or suspected security breach (Severity 0)	Within 4 hours, 24 hours a day, 7 days a week	Support Policy, s3 and s4
Notification of a confirmed security incident affecting Customer Data	Immediately once there are reasonable grounds to believe personal information was compromised (POPIA s21(2)); in every case within 72 hours	DPA, s11
What the notification contains	Nature of the incident; categories and approximate number of people and records affected; likely consequences; remediation steps	DPA, s11
Emergency security maintenance	May be done without prior notice	Support Policy, s8

Reporting a concern. Customers report suspected security issues through the in-platform support portal, marked Severity 0. If the platform is unavailable, use the helpdesk details on xgrcsoftware.com/contact. Security researchers can report a suspected vulnerability to **info@xgrcsoftware.com**, with "Security vulnerability" in the subject.

10 Business continuity and disaster recovery

> If the worst happens, you lose at most an hour of data and are back in service within four hours.

Measure	Commitment
Recovery Point Objective (RPO)	1 hour: the most data that could be lost
Recovery Time Objective (RTO)	4 hours: the longest time to restore service
Backups	Daily full backups, hourly transaction logs, and data replicated across multiple locations
Backup retention	30 days, rolling
Testing	Recovery procedures tested every quarter; results reviewed yearly by our external ISO auditor
Scaling	Resources scale automatically during demand peaks or incidents, protecting the RPO and RTO
Planned maintenance	At least 48 hours' notice for maintenance expected to have material impact (Support Policy, s8)

Business continuity is governed by our Business Continuity Management Policy and is part of the ISO/IEC 27001:2022 certification scope.

11 Supplier, people and physical security

> Security reaches past our own systems: to the suppliers we rely on, the people we employ and the buildings that hold the hardware.

Suppliers

- Every supplier is vetted under our Supplier Security Policy before engagement, including its compliance with POPIA, GDPR and other relevant law.
- Suppliers are reviewed every year as part of our ISMS continual improvement.
- Suppliers that process customer personal information are subprocessors: they sign terms at least as protective as our DPA, and you are notified before a material change.

People

- Everyone who works on XGRC® signs confidentiality and non-disclosure agreements.
- Background checks are carried out on hiring.
- Staff complete security awareness training at least once a year under our Competence, Training and Awareness Policy.

Physical security

XGRC® runs entirely in Microsoft Azure data centres, whose physical security (access control, surveillance, power and environmental protection) is certified under Microsoft's own ISO/IEC 27001 and SOC 2 Type II audits. Our offices are covered by our Physical and Environmental Security Policy.

12 AI governance: MAIA® and AI agents

> AI in XGRC® is governed like any other part of the platform: every interaction is recorded, every agent is limited to what it is allowed to do, and people make the decisions.

- **Audit trail:** MAIA®, the platform's governed AI for business intelligence, data views and intelligent agents, records a full audit trail of AI interactions.
- **Your data and AI models:** Strategix never uses customer data to train AI models. You choose which AI model MAIA® uses: with your chosen provider, that provider's own data terms apply, and we can help you run a local model so prompts and data stay within your own environment.
- **Agent credentials:** Asgard, the XGRC® AI agents platform, keeps upstream API keys and OAuth tokens in an encrypted vault. Agents receive their own scoped keys, tool calls are brokered and filtered, keys can be revoked centrally, and every agent action is logged.
- **People decide:** XLOGIC®, which turns policies and obligations into workflows, lets AI draft proposals but never approve them; every proposal waits for a person.
- **Governing your own AI:** customers can govern their own AI systems in XGRC® AI Governance, aligned to ISO/IEC 42001 and the EU AI Act.

13 Support, maintenance and service levels

> Support targets are contractual, set by severity in the XGRC® Support Policy, with security issues handled around the clock.

Severity	What it means	Initial response	Coverage
0	Confirmed or suspected security breach, or an active vulnerability affecting the platform or Customer Data	Within 4 hours	24 hours, 7 days
1	Complete outage: no user can use the platform	Within 6 hours	Business hours plus on-call escalation
2	A module or major function unavailable	Within 24 hours	Business hours
3	Usable, but a defect needs a workaround	Within 3 business days	Business hours
4	Minor or cosmetic defect	Within 6 business days	Business hours
5	Question or enhancement request	Within 6 business days	Business hours

- **Channels:** the in-platform support portal; the helpdesk on xgrcsoftware.com/contact if the platform is unavailable.
- **Hours:** Monday to Friday, 08:00 to 17:00 South African Standard Time, excluding public holidays; Severity 0 on call outside these hours.
- **Escalation:** unresolved Severity 1 and 2 issues go to senior engineering and management within 24 hours of the first response.
- **Maintenance:** at least 48 hours' notice of maintenance expected to have material impact; urgent security fixes may be applied without notice.
- **Availability:** XGRC® is built for high availability on Microsoft Azure, with load balancing across servers, automatic scaling and the recovery objectives in section 10; service levels for faults are set by severity in the Support Policy.
- **Languages:** the platform runs in English, Portuguese, French and Spanish, with more on request.

14 Shared responsibility and assurance

> Security is shared: we secure the platform, and you control who uses it and what goes into it.

Area	Strategix	Your organisation
Infrastructure, hosting and network	●	
Platform code, patching and vulnerability management	●	
Encryption, backup and recovery	●	
Monitoring and incident response for the platform	●	
Choosing who has access, and with what rights		●
Your identity provider, passwords, MFA and leavers (with SSO)		●
Lawful basis, quality and accuracy of the data you upload		●
Responding to your data subjects (we assist)		●
Integrations and systems you connect to XGRC®		●

Evidence and audit rights

- **On request:** our ISO/IEC 27001:2022 certificate, audit summaries or control statements, subject to confidentiality (DPA, s13).
- **Security questionnaires:** we complete reasonable customer questionnaires; this document answers most standard ones.
- **On-site audits:** not a standard offering; available where law requires or where agreed in writing, subject to confidentiality, security, scope and cost controls.
- **Your own testing:** customer penetration tests by prior written agreement.
- **Internal documents:** ISMS policies are not shared externally, because they contain detail that could weaken our controls (Appendix A lists them).

15 Privacy law: POPIA, PAIA and GDPR

> We act as your operator under POPIA and your processor under GDPR, with a named Information Officer, a published PAIA manual and contractual safeguards for data that crosses borders.

POPIA (South Africa)

Requirement	How we meet it
Operator agreement (s21)	The Data Processing Addendum is the written operator agreement; we process only on your instructions
Security safeguards (s19)	An ISO/IEC 27001:2022 certified ISMS, with the controls in sections 2 to 11
Breach notification (s21(2))	We notify you immediately once we have reasonable grounds to believe your personal information has been accessed or acquired by an unauthorised person, and in every case within 72 hours of confirming an incident
Cross-border transfers (s72)	Data is hosted in the Netherlands under the safeguards in the DPA and applicable law
Data subject rights	We help you respond to access, correction and deletion requests (DPA s10)
Information Officer	Jacob O'Brien; Deputy Information Officers Deneys Minne and Stan O'Brien; paia@strategix.co.za, +27 (0)87 802 0179

PAIA (South Africa)

Our PAIA manual, prepared under section 51 of the Promotion of Access to Information Act, is published at xgrcsoftware.com/legal/paia-manual. It lists the records we hold, how to request access, how we process personal information and how to reach our Information Officer. Requests about your own personal information can also be made through our Privacy Requests page.

GDPR (European Union and United Kingdom)

- **Processor terms:** our DPA meets GDPR Article 28.
- **EU hosting:** Customer Data is hosted in the European Union (Netherlands).
- **Access from South Africa:** for customers subject to GDPR, we sign the EU Standard Contractual Clauses (Module 2 or 3) on request, covering access to data by our staff in South Africa.
- **Breach notification:** without undue delay, as Article 33(2) requires of a processor, and within 72 hours at most.
- **Data protection contact:** our Information Officer, Jacob O'Brien, handles data protection matters under both POPIA and GDPR. We have not appointed an EU representative, as we process EU personal data only as a processor for our customers.

Security partners and personal information

Hakware, which runs our security operations centre and testing, sees only technical security telemetry: no customer data and no personal information. It is therefore not a subprocessor.

16 Frequently asked security questions

> The questions procurement and security teams ask us most, answered in a line each.

Question	Answer	More
Are you ISO 27001 certified?	Yes, ISO/IEC 27001:2022, certified by BSI (IS 804839, valid to 28 August 2027), for the design, development, delivery and support of XGRC®	s2
Do you have a SOC 2 report?	No; our assurance is ISO/IEC 27001:2022 certification. Microsoft Azure, our host, holds SOC 2 Type II	s3
Where is our data stored?	Microsoft Azure, West Europe (Netherlands)	s3
Can our data stay in South Africa?	Not today; Customer Data is hosted in West Europe, with cross-border safeguards under the DPA	s3, s4
Is the platform multi-tenant?	Yes, with strict logical isolation between customers and per-customer encryption keys	s3, s5
Is data encrypted?	Yes: TLS 1.2/1.3 in transit, AES-256 at rest	s5
Do you support SSO and MFA?	Yes: SSO and MFA through Microsoft Entra ID	s6
Can we restrict access by role, site or business unit?	Yes, by module, dashboard and record, and by business unit and category	s6
Do you log user activity?	Yes; record changes are kept in an audit trail	s6
How often do you test for vulnerabilities?	Automated vulnerability assessments and penetration testing daily; a manual penetration test yearly	s7
Do you have 24/7 monitoring?	Yes: Hakware's security operations centre, with SIEM and SOAR	s8
How quickly will you tell us about a breach?	Immediately once we have reasonable grounds to believe your data was compromised; within 72 hours of confirmation at most	s9
What are your RPO and RTO?	RPO 1 hour, RTO 4 hours	s10
Do you test disaster recovery?	Yes, every quarter	s10
Who are your subprocessors?	Microsoft Azure and Microsoft 365, both in West Europe; Hakware sees technical security telemetry only	s4
Will you sign our NDA or DPA?	Our DPA is part of every contract; we review customer terms on request	s4
What happens to our data when we leave?	A copy within 30 days on request; deletion within 90 days; then a Data Destruction Certificate	s4

Question	Answer	More
Do you use our data to train AI?	No	s12
Do you screen and train staff?	Yes: background checks, confidentiality agreements, yearly security awareness training	s11
Do you assess your own suppliers?	Yes: vetted on engagement and reviewed yearly	s11
What is your support response for a security incident?	Within 4 hours, 24/7	s13
Can we audit you?	Certificates and audit summaries on request; on-site audits by written agreement	s14
Can we run our own penetration test?	Yes, with prior written agreement	s14
Is there a mobile app, and is it secure?	Yes, native iOS and Android apps for SHEQX®, with encrypted offline capture	s5
Who is your Information Officer?	Jacob O'Brien, with Deputy Information Officers Deneys Minne and Stan O'Brien; paia@strategix.co.za	s15
Do you have a PAIA manual?	Yes, published at xgrcsoftware.com/legal/paia-manual under section 51 of PAIA	s15
How is EU data protected when accessed from South Africa?	We sign the EU Standard Contractual Clauses on request; data itself stays hosted in the Netherlands	s15
Do you have a DPO or EU representative?	Our Information Officer handles POPIA and GDPR matters; no EU representative, as we act only as a processor	s15
How do we report a vulnerability?	Customers: the support portal at Severity 0. Researchers: info@xgrcsoftware.com, subject "Security vulnerability"	s9

A ISMS documents

> These documents make up our ISO/IEC 27001:2022 information security management system. They are maintained and executed in the XGRC® platform and are not shared externally.

Governance	Policies	Operations and assurance
ISMS Scope Document	Information Security Policy	Risk Treatment Plan
Statement of Applicability	Access Control Policy	Monitoring and Measurement Plan
Information Security Objectives	Cryptography Policy	Internal Audit Programme and Audit Checklist
Roles, Responsibilities and Authorities	Asset Management Policy	Management Review Meeting Minutes

Governance	Policies	Operations and assurance
Risk Assessment and Risk Treatment Process	Supplier Security Policy	Corrective Actions Log
Compliance Obligations and Legal Requirements	Communications Security Policy	Nonconformity and Corrective Action Process
Communication Plan	Physical and Environmental Security Policy	Continual Improvement Process
Documented Information Management Policy	Business Continuity Management Policy	Operational Planning and Control Document
Competence, Training and Awareness Policy	Information Security Incident Management Policy	Incident Management Policy
	System Acquisition, Development and Maintenance Policy	

B Related documents

> All published in the XGRC® Trust Centre, xgrcsoftware.com/trust.

Document	Reference	Address
Cybersecurity & Data Protection Policy	XGRC-SEC-002	xgrcsoftware.com/trust/cybersecurity-data-protection-policy
Data Processing Addendum	XGRC-DPA-002	xgrcsoftware.com/legal/data-processing-addendum
Support Policy	XGRC-SUP-002	xgrcsoftware.com/legal/support-policy
Subprocessor List	v2.0	xgrcsoftware.com/trust/subprocessors
Data Hosting	v2.0	xgrcsoftware.com/trust/data-hosting
Privacy Policy	v2.2	xgrcsoftware.com/legal/privacy-policy
Acceptable Use Policy		xgrcsoftware.com/legal/acceptable-use-policy
End User Licence Agreement		xgrcsoftware.com/legal/end-user-licence-agreement
PAIA Manual	v1.03	xgrcsoftware.com/legal/paia-manual
Privacy Requests	v2.0	xgrcsoftware.com/legal/privacy-requests
ISO/IEC 27001:2022 certificate (BSI)	IS 804839	Verify in BSI's certificate directory

QUESTIONS, QUESTIONNAIRES AND EVIDENCE

Talk to us about security

EMAIL

info@xgrcsoftware.com

PHONE

+27 (0)87 802 0179

TRUST CENTRE

xgrcsoftware.com/trust

INFORMATION OFFICER

paia@strategix.co.za

SYNERGY IN ASSURANCE, STRENGTH IN COMPLIANCE®

DRIVING COMPLIANCE®

Strategix Application Solutions (Pty) Ltd, the developer and operator of XGRC® Software. XGRC®, SHEQX®, MSX®, MSXCyber®, ENVIRX®, MAIA® and XLOGIC® are registered trade marks of Strategix Application Solutions (Pty) Ltd. This document describes our security programme as at October 2026; contractual commitments are those in the documents it references.