Leesman®

Policy Information: Security Statement	
Company	Leesman, Data Processor.
Scope of policy	This policy outlines Leesman's stance on Infosec. It is deliberately high level to retain the confidentiality of Leesman policies. It can be read alongside the Leesman Information Security Management Policy.
Data category subject of this policy	Any individual.
Policy prepared by	CTO
Date approved by CEO	Yes
Policy review date	29th September 2022, by Fanny Mrani.

Leesman

Leesman Security Statement

This document is a non-confidential, public facing, high level document outlining Leesman's stance on Infosec. It is deliberately high level to retain the confidentiality of Leesman policies. It can be read alongside the Leesman Information Security Management Policy.

This Security Statement applies to the products, services, websites and apps offered by Leesman except where otherwise noted. These products, services, websites and apps are collectively named as the "services" in this Statement. This Security Statement should be read alongside other user agreements presented to Leesman clients.

Leesman values the trust clients place in us by letting us act as processors of their data. We take our responsibility to protect and secure client information seriously and strive for complete transparency around our security practices detailed below. Our Privacy Policy also further details the ways we handle your data.

Physical Security

Leesman's information systems and technical infrastructure are hosted within AWS, world-class, SOC 2/3, ISO 27001 accredited data centres.

Compliance

Leesman complies with GDPR and DP2018. We are CyberEssentials+ accredited and B-corp certified.

Access Control

Access to Leesman's technology resources is only permitted through secure connectivity and in most cases, requires multi-factor authentication. Our production password policy requires complexity, expiration, and lockout and disallows reuse. Leesman grants access on a need to know on the basis of least privilege rules, reviews permissions quarterly, and revokes access immediately after employee termination.

Security Policies

Leesman maintains and regularly reviews and updates its information security policies, at least on an annual basis. Employees must acknowledge policies and undergo additional training both formal and ad-hoc and job specific security and skills development and/or privacy law training for key job functions. The training schedule is designed to adhere to all specifications and regulations applicable to Leesman.

Personnel

Using recruiters or consultants, Leesman conducts background screening at the time of hire (to the extent permitted or facilitated by applicable laws and countries). In addition, Leesman communicates its information security policies to all personnel (who must acknowledge this) and requires new employees to sign non-disclosure agreements and provides ongoing privacy and security training.

Leesman

Dedicated Security Personnel

Leesman also has a dedicated Technology team, which focuses on application, network, and system security. This team is also responsible for security compliance, education, and incident response.

Vulnerability Management and Penetration Tests

Leesman maintains a documented vulnerability management program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. All networks, including test and production environments, are regularly scanned using trusted third-party vendors. Critical patches are applied to servers on a priority basis and as appropriate for all other patches.

We also conduct regular internal and external penetration tests and remediate according to severity for any results found.

Encryption

We encrypt your data in transit using secure TLS cryptographic protocols. Leesman client data is also encrypted at rest.

Development

Our development team employs secure coding techniques and best practices, focused around the OWASP Top Ten. Developers are formally trained in secure web application development practices upon hire and annually.

Development, testing, and production environments are separated. All changes are peer reviewed and logged for performance, audit, and forensic purposes prior to deployment into the production environment.

Asset Management

Leesman maintains an asset management policy which includes identification, classification, retention, and disposal of information and assets. Company-issued devices are equipped with full hard disk encryption and up-to-date antivirus software. Only company-issued devices are permitted to access production networks.

Information Security Incident Management

Leesman maintains security incident response policies and procedures covering the initial response, investigation, client notification (no less than as required by applicable law), public communication, and remediation. These policies are reviewed and tested annually.

Leesman

Breach Notification

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Leesman learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under UK/GDPR laws and regulations, as well as any industry rules or standards applicable to us. We are a member of ICO. We are committed to keeping our clients fully informed of any matters relevant to the security of their account and to providing clients all information necessary for them to meet their own regulatory reporting obligations.

Information Security Aspects of Business Continuity Management

Leesman's databases are backed up on a rotating basis of full and incremental backups and verified regularly. Backups are encrypted and stored within the production environment to preserve their confidentiality and integrity and are tested regularly to ensure availability.

Your Responsibilities

Keeping your data secure also requires that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems when hosting, disseminating survey links. We offer TLS to secure the transmission of survey responses.

Logging and Monitoring

Application and infrastructure systems log information to a centrally managed log repository for troubleshooting, security reviews, and analysis by authorised Leesman personnel. Logs are preserved in accordance with regulatory requirements. We will provide clients with reasonable assistance and access to logs in the event of a security incident impacting their account.

For more information, please contact one of the below:

- Technical Onboarding Specialist

Fanny Mrani, fanny.mrani@leesmanindex.com

- Chief Technology Officer & Data Protection Officer

Allen Green, allen.green@leesmanindex.com