Our Data Security Policy

Last updated: 28 September 2023

Data security is of paramount importance to Arctic Shores. Businesses use Arctic Shores' behaviour-based assessment secure solution with confidence to see their candidates' truest potential beyond their Curriculum Vitae to build the extraordinary teams they ne

How We Keep Data Secure

Arctic Shores have a dedicated team of security, compliance, and privacy experts to ensure we have the appropriate policies, processes, and standards in place to ensure that the data we process is secure and in accordance with relevant legislation.

Arctic Shores Security Culture

Employee Screening	Arctic Shores has created a strong security culture for all employees This starts during the hiring processes, employee onboarding and as part of ongoing training. Arctic Shores performs verification checks on all candidates for employment in accordance with relevant laws, regulations, and ethics. All candidates have reference checks from previous employment, adverse financial checks, identity and eligibility to work verification The extent of these checks are dependent on the position Arctic Shores may also conduct professional qualification verification and criminal check.
Security Awareness Training	All Arctic Shores Employees receive Information Security Awareness training during the onboarding process and monthly during their time at Arctic Shores. Some employees will also undertake further security training that is specific to their role.

Building Security

Manchester Office	Security guards are present on site. Entry to the building and office is via security card. CCTV (24/7) is in place. There is a full visitor process in place.
London Office	There are two manned receptions and security guards are present on site. Entry to the building and office is via security card. CCTV (24/7) is in place. There is a full visitor process in place.

Personal Data

Candidate data

When a candidate is invited to take our behaviour-based assessment, the below personal data will be collected to support the simple management of the service: -

- Name
- Email Address
- IP Address
- Client ID
- psychometric assessment results

Demographic data is optionally collected directly from the candidate to support equal opportunity rights and includes the collection of ethnicity and health information which is sensitive data.

It is possible to use this solution without providing personal data and purely providing a client ID for each candidate.

Client Account Administration	Personal data that is collected to administrate client programmes: • Name • Email Address • IP Address
Data Protection	We work in accordance with data protection laws and follows good practice. protect the rights of employees, customers and partners, are open about how we store and process individuals' data and protect ourself from the risks of a data breach.
Data Retention	We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for. We retain our anonymised research datasets beyond the end of this period, but once we have deleted your identifying details candidates can no longer be identified, and the research data does not constitute personal data.

Access Control

Role Based Access Control	Arctic shores functions on the principles of least privilege and role-based permissions to mitigate the risk of data exposure in line with ISO 27001 access management requirements.
Login Credentials	Access to the solution is based on username, strong password, based on a defined password policy. Two factor authentication is also in place.

Data Security

	Arctic Shores behaviour-based assessment is a Software as a Service solution.
Data Centres	Our infrastructure is hosted in geographically redundant locations in AWS Ireland. AWS possesses all necessary internationally recognised certifications and accreditations and complies with rigorous international standard. These include ISO 27001 for technical measures, ISO 27018 for cloud privacy and SOC 2 Type I and Type 2 compliant.
Network Segmentation	Our SaaS network is segmented at each layer to ensure appropriate security controls and monitoring is in place.
Software Development	Arctic Shores follow best practice in respect of coding standards, source control, code review and testing. Our development has a security focus in respect of our training, our software frameworks with built in security, and our reference to the OWASP code review project.
Encryption at rest	All customer data is encrypted at rest using the industry standard AES-256 encryption algorithm.
Encryption in transit	All customer data in transfer is protected by strong encryption protocols. The severs are mandated to make use of Transport Layer Security encryption with strong ciphers.
Patching	All information assets, either owned by Arctic Shores or those in the process of being, is manufacturer supported and have up-to-date and security patched operating systems and application software.

Logging	Log files are centrally aggregated and subject to continuous monitoring. The log files are retained for 6 months.
Back Up	Backup processes undertaken by Arctic Shores are to utilise approved hardware, software, and other supporting tools for ensuring the confidentiality, integrity, and availability of the entire backup platform. Our backup is encrypted and hosted in geographically redundant locations on Amazon Web Services. Backups are kept for 6 months.
Business Continuity	A business continuity plan, which includes disaster recovery, is developed for each system or activity within Arctic Shores. The nature of the plan and the actions it contains are commensurate with the criticality of the system or activity to which it relates. Business continuity and disaster recovery are tested twice a year.

Vulnerability Control

Vulnerability Management	Pen tests take place on an annual basis and vulnerability scans take place on a quarterly basis.
Patching	All information assets, either owned by Arctic Shores or those in the process of being, is manufacturer supported and have up-to-date and security patched operating systems and application software.

Mobile Device Management	All our employees' machines and laptops use mobile device management to ensure that each device is set up in a secure manner.
Enterprise Antivirus	All our employees' machines and laptops are set up with an enterprise antivirus solution.

Incident Response Process

Incidents	Our incident response process ensures that threats to our estate, incidents to the confidentiality, integrity and availability of the data and vulnerabilities are identified, reported, analysed, contained, and resolved. In the unlikely event of a data breach, we will inform our clients within 24hr of becoming aware of the incident and provide a data breach incident report.

Information Security Policies

Information Security Policy	Arctic Shores has a full suite of ISO 27001 compliant Information Security policies and processes in place. The Information Security policy is our overarching Information Security Policy. It provides a framework for the management of information security throughout Arctic Shores.

Third-Party Services

Third-Party Management	The procurement of new or renewing services with third parties go through our third-party management assessment process.
Amazon Web Service	Our solution and backup are hosted in an EEA AWS data centre. The data centre is ISO 27001, ISO 27018, SOC 1 Type II and SOC 2 Type II certified. We make use of AWS email to provide us with an SMTP service.
Zoho Services	Hosted in The Netherlands, backed up in Ireland and technical support is provided by India. GDPR compliant data transfer processes are in place. Zoho collects our survey information, where pseudonymised demographic data is optionally collected.

Certifications and Compliance

ISO 27001 Certified

Arctic Shores is ISO 27001 certified. We have a mature information security management system in place to ensure that the appropriate controls to protect information are implemented within the business. ISO 27001 compliant policies and procedures ensure all data is treated appropriately, securely and in line with business requirements, laws and regulations. These policies are reviewed on an annual basis, or when a significant change occurs.

Our risk management framework defines our assessment and treatment of information risks within the business, in line with the ISO/IEC 27001 standard.

GDPR Commitment

Arctic Shores is proud to comply with the GDPR, UK GDPR and Data Protection Act 2018, as well as other regulations and laws that impact our business.

Previous versions:

nil.