We are on the same team!

We understandably receive a lot of questions from our customers as to how Preservica is taking appropriate action for the protection and confidentiality of our client data as a cloud service provider.

The responsibilities detailed in this paper are applicable across our whole service offering but are specifically written in the context of Preservica Cloud.

At a high level, Preservica handles security of the applications themselves, the systems they run on, and the environments those systems are hosted within. We ensure your systems and environments are compliant with relevant standards, including ISO 27001:2013, Cyber Essentials Plus and SOC2, as required.

You, our clients, manage the information within your accounts, the users and user accounts accessing your data and the management of records within the application. When using our services, you are responsible for ensuring your business is meeting your own compliance obligations.

In the cloud, the security of your data on our services is a joint responsibility. We developed these shared responsibilities to outline what actions we take to protect your data, and what you need to do.

	What we do	What you need to do
Governance, Risk and Compliance	Ensure Preservica has established and tested business continuity and incident response plans. Ensure our data centre partners meet or exceed Preservica's compliance requirements. Provide information about our compliance through our Trust Center. Ensure our offerings meet or exceed the certifications and accreditations that we claim. This includes ISO 27001:2013, SOC 2 Type II and more. See our Trust Center. Adhere to our Sustainability Charter to ensure our continued success as a business.	Operate within the law of the jurisdiction in which you operate. Assess the suitability of our services based on the information we provide. Understand the risks associated with using a SaaS service as well as the benefits.

PRESERVICA SHARED RESPONSIBILITY MODEL

	What we do	What you need to do
Infrastructure	Provide you with access to our services according to our SLA. Ensure that our infrastructure is configured with appropriate network security technologies.	Understand that Preservica operates on cloud infrastructure provided by a 3rd party (AWS or Azure). Ensure suitable endpoint protection is in place on the devices you use to access Preservica.
Data	Access your data only if there is a specific need to do so. Notify you of any breach we become aware of that affects your data. Maintain backups and recovery plans to meet our RPO and RTO objectives. Ensure your data is encrypted at-rest and in-flight. Ensure the integrity of data that you ingest through checksums and other cryptographical techniques.	Understand the regulatory and compliance needs of the data you wish to ingest. Only ingest data that is permitted given the compliance of the Preservica service. Ensure your staff are aware of their obligations under the Acceptable Use Policy. If you choose to use a custom domain to access the service, you may need to collaborate with our Operations team for SSL certificate renewals. Manage the data and metadata that you ingest into the service according to your organizations data and records management policies.
Security Operations	Manage security incidents and notify you of any incidents that affect your environment. Receive and manage vulnerability reports related to our service. Monitor our platform for bad or malicious actors.	Monitor your user accounts and activity logs for malicious activity. Be aware of the risks of social engineering, phishing and other attack vectors that could result in your users inadvertently revealing their log in credentials.
Application Security	Develop and deploy security tools and functionality that empower you to manage users, roles and permissions effectively. Remediate any vulnerabilities in the service in a timely manner using a risk-based approach.	Configure and manage roles according to your business needs. Configure access control and other security controls according to your own security policies. Add, delete, modify, and periodically review users of the service according to your security policies. Notify Preservica of any unauthorized use of your organization accounts.