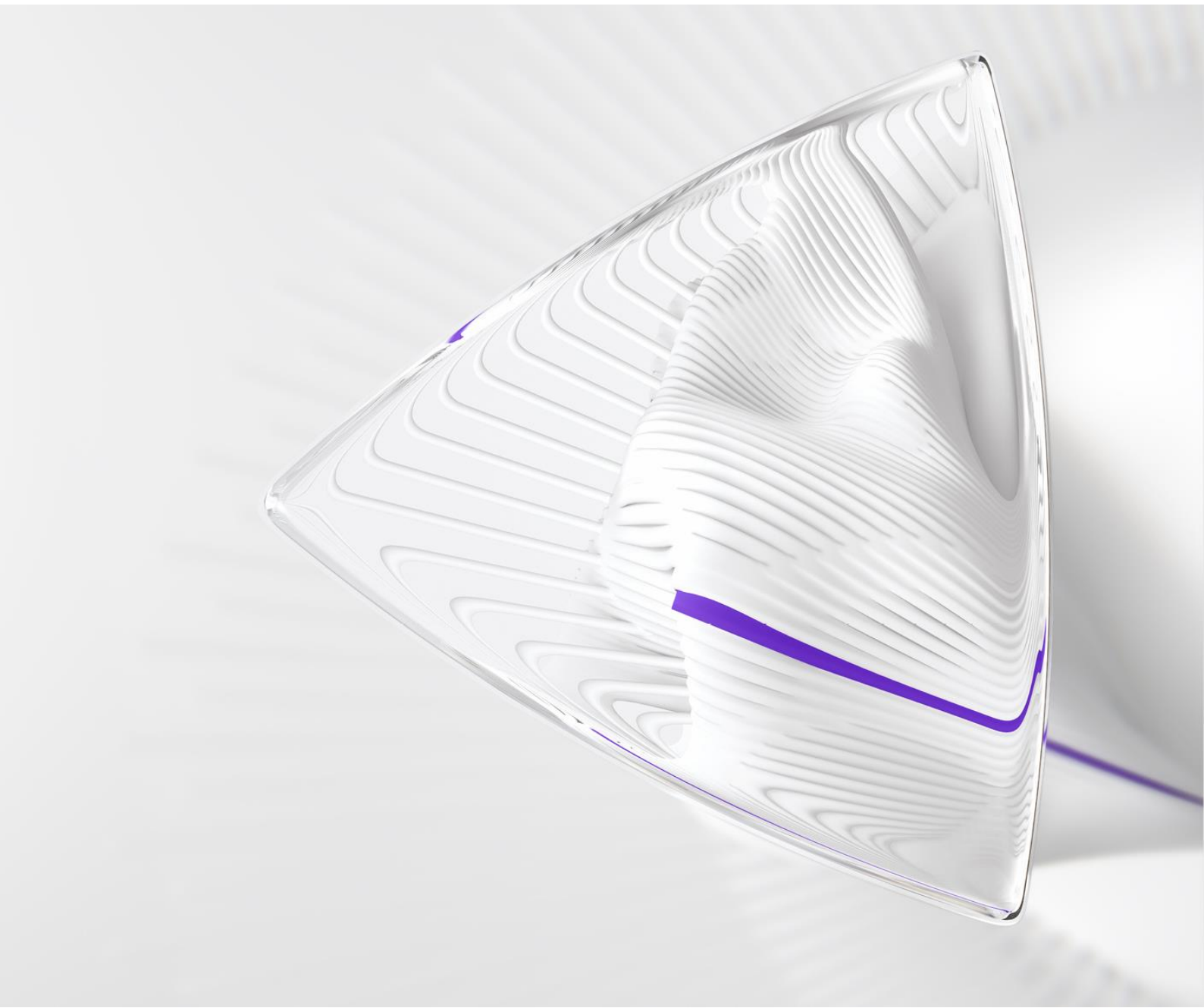
Clarivate™

# Information security program overview



Clarivate is committed to its Information Security Risk Management program, and our charter is approved by our Executive Committee. We have an extended team of certified security subject matter experts located globally and dedicated to the security of our services.

# Our commitment

**We use a risk-based approach to address our compliance requirements by ensuring alignment with business priorities and customer needs. We achieve this through policies, standards and supporting security controls at a level appropriate to the service being provided.**

Additionally, we ensure appropriate security controls are communicated to application owners and technology teams across the business for the secure development of products and a secure operating environment. We make it our priority to mitigate threats to the confidentiality, integrity and availability of our data and the customer data which we store, process or transmit.

Clarivate employs individuals who are trained to identify issues and resolve them as quickly as possible with minimal impact on its customers. Our involvement in industry, government forums and groups is also a demonstration of our proactive approach to understanding and proactively mitigating the threats we encounter in the course of providing robust applications and services to our customers.

# Our approach

**We have implemented a set of information security policies and standards outlining information security and risk management principles that apply to our staff, processes and technology practices for deploying and maintaining our information systems.**

Additionally, we focus on continuous improvement by reviewing and adapting our policies and standards to address the many aspects of our products and services, evolving threats, regulatory changes and our customers' requirements for information security.

Our policies and standards are aligned with widely accepted international standards to provide global assurance of practices that ensure the confidentiality, integrity and availability of our products and services.

Our planned certification and assurance programs such as the ISO 27001 standard and SSAE18 SOC2 assurance report further demonstrates our commitment to a secure operating environment.

Product assurance standards are integral elements in the development of our products. Our product development teams regularly consult with our information security subject matter experts to ensure data security is built into their applications and services.

In addition, our Information Security team supports a comprehensive application security testing capability including services to perform static and dynamic application security testing and third-party penetration testing. This program also provides mandatory training for development staff in the secure design and coding and testing of their applications.

# Information security risk management

**Our information security risk management practices are established upon a risk management framework which implements and reviews applicable policies and standards, aiming at continuous improvement.**

## Our staff

All our staff are subject to our code of conduct encompassing our company's values and mission. They are made aware of their responsibilities, our policies and standards and receive regular guidance and support from our Information Security team on best practices relating to data security.

We conduct mandatory information security training on an ongoing basis and provide supplemental training to specific target groups and individuals as required. Our staff are bound by obligations of confidentiality and understand the consequences for failing to adhere to our policies and their responsibilities.

## Infrastructure security

Our services are offered through public and private networks. Communications are protected against eavesdropping by secure channels, and strong encryption. Access to production servers require MFA (multi factor authentication). Activities are logged and monitored. There are tiered controls, including the use of network segmentation, to ensure the appropriate level of protection to systems and data. Data Loss Prevention controls are also deployed for email security.

## Endpoint and virus protection

In line with our policies, all Clarivate owned and supported operating systems which are hosted in our data centers or deployed in the cloud are required to be configured with our antivirus solution.

## Patch management

We gather and review security threat intelligence from our internal vulnerability management tools, vendors and other third-party security organizations. Our patch management standard provides appropriate patching practices to our technology teams. At times, additional security controls may be implemented to provide mitigation against known threats.

## Security monitoring

Automated and systemic centralized security logging and monitoring of the operating environment is ongoing through our SOC (Security Operation Center) for the purpose of real-time awareness, event correlation and incident response.

## Incident response

An incident response process is in place to address incidents as they are identified. Incidents are managed by a dedicated incident response team which follows a documented procedure for mitigation and communications. The plan is implemented according to various recognized standards and industry best practices such as: 1) NIST Computer Security Incident Handling Guide, 2) VERIS Community Database (VCDB) and 3) Verizon Data Breach Investigations Report (DBIR).

## Device lockdown

Standard security builds are deployed across our infrastructure with our security agents installed. Our server builds are based on industry practices for secure configuration management.

## Capacity management and monitoring

Monitoring of systems, services and operations are implemented to ensure the health of our operating environments. Management tools are implemented to monitor and maintain an appropriately scaled and highly available environment.

## Vulnerability scanning

Our Information Security Team supports a vulnerability scanning and policy compliance service that product and technology teams utilize for internal and external vulnerability scanning and configuration compliance. Internet-facing sites on our global network are periodically scanned as a practice in our program focused on vulnerability management.

## Risk assessment methodology

Our product and technology teams engage information security subject matter experts regularly to provide risk assessments services. Architecture reviews, external vulnerability scans, application security testing and technical compliance reviews are several of the services performed during risk assessment activities.

Following risk assessment activities our Information Security Risk Management team consults with product and technology teams to develop remediation plans and roadmaps to address gaps in compliance, or areas of identified risk.

Additionally, our IT Governance, Risk and Compliance team performs audits against policies, standards and regulatory requirements, and registers findings for review and remediation initiatives within the business.

## Physical security and third-party vendor management

All strategic data centers including cloud service providers where the majority of application products are deployed and managed to the standards, and industry best practice that Clarivate has adopted. Our guidelines include requirements for physical security, building maintenance, fire suppression, air conditioning, UPS with generator back-up, and access to diverse power and communications. Clarivate reviews third party data centers assurance reports as part of our Vendor Risk Management program.

A variety of secure methods are used to control access to our facilities. Depending on the sensitivity of the facility, these methods may include some or all of the following: the use of security staff, ID cards, electronic access control incorporating proximity card readers, pin numbers or biometric devices.

For information about our products visit: **clarivate.com**

Contact us: **clarivate.com/contact-us**


© 2020 Clarivate