Clarivate™

Information Security Program Overview

Contents

Introduction

At Clarivate, we understand the importance of adopting industry-leading security practices and technology needed to protect customers' data. Our security practices are embedded across all our technology, programs and processes.

Clarivate has adopted the International Standards Organization (ISO) 27000 family of standards – ISO/IEC 27001:2013 as the basis for its Information Security Management System and established, documented, implemented all policies, standards and controls which conform to the requirements of ISO 27001 Security Standard.

Where applicable and where in scope, Clarivate undergoes External Surveillance assessments from an accredited certification body on an annual basis to verify compliance against the controls defined in ISO 27001:2013 and AICPA SOC 2 standard.

In this document, we provide an overview of our security program and controls, and how our corporate values drive our commitment to excellence in securing customers' data. The content of this document encompasses the aspects of Administrative, Physical, Environmental and Technical (Network and Systems Security) controls that enable Clarivate to build robust processes that strengthen our customers' trust to deliver high levels of integrity, confidentiality, and availability of data.

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.

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 Program

Clarivate has a well-defined Information Security Program aligned to well-known industry standard ISO 27001 to protect the confidentiality, integrity and availability of its information assets.

Personnel

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.

In accordance with relevant laws and regulations, adequate background verification checks are performed while recruiting an individual as permanent staff to ensure the authenticity of the individual and to reduce the possibility of threat to critical information assets.

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.

An Employee exit process is followed at Clarivate which involves revocation of system permissions/access rights and return of company assets in a timely manner.

User Access management

Clarivate has a well-defined process for granting access to all information assets. Privileges and access rights are granted to employees based on "Need-to-know" and "Least-privilege" principles to protect information assets against unauthorized access and disclosure. Clarivate password policy is enforced across the board on all information assets, which ensures a minimum length, complexity, password expiry, history and account lockout requirements in case of failed attempts.

Infrastructure security

Our services are offered through public and private networks. Communications are protected against eavesdropping by secure channels, and strong encryption. Clarivate has secured its perimeter with state of art Network Intrusion Prevention Systems (NIPS), Application Firewalls and Network based Firewalls.

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 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).

Clarivate's Incident Response process requires incidents to be effectively reported, investigated, and monitored to ensure that corrective action is taken to control and remediate security incidents in a timely manner.

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.

Operations Security

Clarivate ensures all changes to operating information systems environment which includes changes to servers, network equipment and software are subject to formal change management process.

Clarivate ensures backup copies of information and software are maintained for data recovery in case of events such as system crash or accidental deletion of information.

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

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 most of applications and 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 to ensure that access is only gained in a controlled way on an operational needs basis. 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, physical locks and pin numbers.

About Clarivate

Clarivate™ is a leading global information services provider. We connect people and organizations to intelligence they can trust to transform their perspective, their work and our world. Our subscription and technology-based solutions are coupled with deep domain expertise and cover the areas of Academia & Government, Life Sciences & Healthcare and Intellectual Property. For more information, please visit clarivate.com.

Contact our experts today:

clarivate.com/contact-us

clarivate.com

Document Version : 3.0
Document date : 8 August 2023
Classification : Public