Data & Information Security

v2.5 June 2020

Data Information & Security

Hundreds of companies have trusted Lytica with their data. We employ best-of-breed proactive security practices, encryption and intrusion detection methods to ensure customer data is always protected.

We protect your information, while maintaining the integrity of our information service offering. We rely on industry best practices, robust security infrastructure and comprehensive policies to protect our data, along with that of our clients and partners.

Some of the ways Lytica protects your information are listed below:

Data Centers & Servers

Physical Security: Lytica's information infrastructure is hosted by OVH, which hold numerous certifications including PCI-DSS, SOC 1, ISO 27001, ISAE-3402, SSAE-16 Type 1, and SOC 2 Type 2. Power, and internet connectivity are monitored and guaranteed by the facilities providers.

Remote Monitoring: All production network systems, networked devices, and circuits are constantly monitored and logically administered by Lytica staff.

Patching and Maintenance: System security patches are applied monthly.

Anti-Malware: All servers are protected using industry-recognized endpoint protection software.

Network Security

Intrusion Detection and Prevention: We employ state of the art Network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to detect, prevent and mitigate potential security events.

Architecture: Lytica's network architecture is designed to ensure that customer data is isolated from edge network traffic. There is a hard air-gap between any customer supplied data and Internet facing Lytica platforms. All data is processed within Lytica's inner network, and only aggregated, fully anonymized information is used for report generation.

Network Vulnerability Scanning: Lytica performs comprehensive vulnerability scans to monitor network and endpoint security. These are carried out on an ongoing basis.

Security Incident Event Management (SIEM): Lytica uses an industry recognized SIEM solution to monitor, detect and respond to security incidents.

Network Access: Access to the Lytica network is restricted to authorized users and devices.

Application Security

Data in Transit: Internet communications are encrypted via Secure Hypertext Transfer Protocol (HTTPS), Secure File Transfer Protocol (SFTP) and Transport Layer Security (TLS).

Data at Rest: Customer data is secured using Advanced Encryption Standard (AES).
Separate Environments (QA, DEV, UAT, PROD): Development, testing and staging environments are separated from the production environment, both physically and logically.

Penetration Testing: Web and network penetration tests on the application are performed every six months by internal teams.

Application Vulnerability Scanning: An automated vulnerability scan is run on every code release before it is pushed to user acceptance testing (UAT) environments. If the penetration test fails, the release and relevant information are sent back to development.

Secure Operations

Security Incident Response: Lytica has a documented incident response plan that covers all aspects of an incident, from detection to post- incident analysis. Our plans follow the guidance of the ISO 27001 standards.

Disaster Recovery / Backups: Lytica has policies, tools and procedures in place to ensure minimal disruption in the event of a disaster. We employ industry standard containerization methodologies to monitor, and rapidly 'factory reset' stressed infrastructure elements. Customer configuration and report data is replicated to a secondary site that is available if the primary site goes offline. We test the disaster recovery plan annually.

308 Legget Drive
Ottawa, Canada
K2K1Y6
sales@lytica.com

LYTICA®

Data & Information Security