dynata

Information Security Overview

Dynata recognizes the importance of data privacy and data security and has established an Information Security program to manage Dynata's data security requirements and constantly monitor developing trends and threats. The program is led by qualified information security professionals who closely collaborate with Dynata's General Counsel to ensure that any contractual or regulatory data protection requirements are integrated into the Information Security program. The Information Security team leverages all the necessary departments and staff at Dynata to address security issues as they arise. Dynata maintains AICPA SOC2 compliance with Security and Privacy Criteria as part of its Information Security program and is ISO 27001:2022 Certified. A high-level overview of the technical, physical, and administrative safeguards that Dynata has implemented to protect customer data are described below.

Information Security Policies and Standards

Dynata's Global Information Security Policies and Standards address the information security areas that are critical to Dynata. These policies and standards are approved by management and communicated to all employees and/or contractors.

THESE POLICIES COVER

- Dynata's Information Security Policy
- Acceptable Use
- Confidential Information
- Global Privacy and Data Protection
- Global Data Classification and Handling
- Account Security
- Risk Management
- Network Security
- Physical Security
- Technical Vulnerability Management
- Vendor Risk Management

Information Security Awareness Training

Information Security Awareness training is required to all Dynata employees upon hire and on an annual basis. The requirement to adhere to organizational policies is addressed and communicated in the Dynata employee handbook. Contractors and third party users must agree to abide by Dynata Information Security policies prior to gaining access to Dynata information systems.

Dynata employees receive training on safe handling of customer data, including:

SECURE METHODS OF DATA TRANSMISSION AND STORAGE

SECURE PRACTICES FOR HANDLING OF PAPER AND ELECTRONIC ASSETS

SECURE PRACTICES FOR COMMUNICATING ORAL INFORMATION

Background Checks

In the United States, prospective new hires undergo a background check that includes a seven (7) year history, as permitted by law, to ensure compliance with applicable client agreements and ensure a safe workplace for its employees. Dynata does not hire individuals with felony convictions and/or criminal convictions for crimes involving fraud/dishonesty.

Data Center Security

Dynata systems are located in third party full service co-location facilities which provide state-of-the-art security that meet a number of compliance and/or third party certification standards including ISO 27001:2013, NIST 800-53, SOC2 and/or SSAE 16. These facilities provide redundancy with multiple backup generators, uninterrupted power supplies and air conditioning units. Physical security controls include perimeter fencing, surveillance, on-site security guards, key card access, biometric systems, and mantraps to control and restrict access to data centers. Security cameras are placed throughout the data center facilities to record physical activity and are actively monitored 24/7/365.

Office Security

Physical security requirements for Dynata offices are communicated to the organization via employee training and company policy. While offices have varying levels of security, the objective for all offices is to prevent unauthorized access to Dynata information systems and any data that is housed at the facility. Physical safeguards include: badge access, keys, fencing, gates, receptionist/security personnel, security patrols, visitor logs, biometrics, pin/key-based locks. Some offices have cameras.

Network Security

A network security policy has been published and communicated that outlines Dynata's requirements for network security. The following network security controls are implemented:

External networks (Internet, extranets, external partners) are segregated from internal networks with firewalls

Internet facing servers and services are located in the DMZ network with firewalls in-between

Firewalls are configured to deny all inbound connections by default and only allow those based on application/system needs

Firewall rules are regularly reviewed

Network-based Intrusion Detection and Prevention systems are deployed at the network perimeter

Internal network traffic is monitored for malicious activity with passive vulnerability scanners

Firewall logs are sent to a log aggregation/correlation tool to detect indicators of compromise or other malicious network activity

Traffic is encrypted using HTTPS

Remote access to the Dynata network is limited by hardware firewalls and available to select employees through VPN access. Security features include multi-factor authentication and encryption utilizing HTTPS

Threat Management

Dynata has an IT Risk Assessment Program that includes:

- Weekly external and internal vulnerability scans
- Annual independent network security assessments and a penetration tests
- Standard practices for assessing server vulnerability and remediation prior to moving those servers to production

Security Monitoring

Dynata has a security monitoring strategy with specific use cases to monitor for real-time cyber events, for example:

- Intrusion detection
- Ransomware detection
- Virus detection
- Critical group or infrastructure changes
- Rogue AP detection
- Detections for indicators of compromise
- Detections for anomalous activity

Encryption

As part of the Dynata Information Security Policy, encryption is used to protect information in transit and at rest. Dynata employees are required to work with IT Operations and Information Security teams to ensure the method of data transmission for certain data types will utilize an acceptable encryption algorithm. When transmitting data with clients, Dynata recommends the use of its internally hosted secure transport system, which utilizes SFTP and HTTPS for file transmission.

Data Destruction

When data is scheduled to leave organizational control (e.g., the disposal of assets), Dynata engages third parties for the disposal of equipment and works with vendors that comply with the requirements of NIST Special Publication 800-88 and provide certificates of destruction. Any specific requirements for the secure disposal of data is determined on a project-by-project basis as set forth by each specific client.

Additional Controls include:

- Routine encrypted backups
- Disaster Recovery for core systems
- Audit log management
- Change Management
- Controls against Malware (e.g., Anti-Virus, Web Filtering)
- Access Control
- User registration, modification and de-registration procedures
- Password policies
- Management of privileged access rights
- Review of user access rights
- Software Development Lifecycle

Independent Review of Information Security

Additional details about Dynata's Information Security Program can be provided following the execution of a mutual Non-Disclosure Agreement (NDA) by both parties. A more detailed vendor risk assessment questionnaire can be completed by providing the document and instructions to your Dynata business partner.