CIS Group

Data Protection Measures

1.Introduction

CIS Group is a leading North American provider of business software solutions, specializing in Direct Store Delivery (DSD), Sales Force Automation (SFA), and transportation management for both people and freight. With a legacy dating back to 1977, ***CIS Group*** has built a reputation for delivering innovative, secure, and scalable digital tools that empower organizations to optimize operations and drive productivity.

As a trusted technology partner to a wide range of industries, ***CIS Group*** recognizes the critical importance of safeguarding customer data and maintaining the highest standards of information security. This document outlines the comprehensive data protection measures implemented across the organization to ensure the confidentiality, integrity, and availability of information assets. These controls are aligned with industry best practices and regulatory requirements, including ISO 27001 and Québec's Law 25, and are continuously reviewed and enhanced to address evolving threats and business needs.

2.Organizational Controls

To ensure a robust and resilient information security posture, ***CIS Group*** has implemented a comprehensive set of organizational controls. These controls are designed to establish clear governance, enforce accountability, and align security practices with business objectives and regulatory requirements. The following table outlines the key categories and specific measures that form the foundation of ***CIS Group***'s security organization, policy management, and data protection strategy.

Category	Controls
Security Organization	***Security Structure*** • An established information security structure exists with clearly defined roles and responsibilities, aligned with the segregation of duties principle. Regular meetings of the Information Security Steering Committee are conducted. • Management requires all employees and consultants to acknowledge and sign ***CIS Group*** security policies and standards.
Security Policy and Procedures Management	***Security Policies, Standards and Procedures*** • A complete information security documentation exists and is operationalized (policies, standards, plans, guidelines, operating procedures, etc.). • A documentation management process (creation, maintenance, review, decommissioning) is in place.
Assets and Data Protection	***Assets Management*** • An asset management tool is used to maintain a hardware and software asset inventory. • There is a defined process for equipment return and secure decommissioning (including data sanitization and physical destruction). • Policies on Acceptable Use and Information Classification ensure proper handling of information and assets. Only employee laptops are permitted to leave the office. • Physical documents are no longer used, supporting a fully digital and secure workspace. ***Data Security*** • All workstations have full disk encryption enabled. • Data in transit between ***CIS Group's*** environment and all authorized devices and resources (laptops, mobile devices, servers, applications, etc.) is encrypted.

Category	Controls
Risk, Compliance and Supplier Management	***Risk Management*** • An information security risks management process is implemented and operationalized. • Risks are assessed, treated, and regularly communicated and monitored. ***Compliance Management*** • A Data Protection Officer is assigned to ensure compliance with Québec Law 25 and other privacy regulations. • Access to resources containing sensitive information or PII is restricted. ***Supplier and Third-Party Management*** • Supplier and third-party risks are integrated into the information security risk management process, with due diligence conducted for new or changing services. Contracts always include specific information security clauses and requirements. • A Cloud Security Standard is implemented, ensuring security requirements are met and controls are in place to secure cloud environments. ***Independent Audits*** • Regular penetration tests are performed on ***CIS Group's*** environment and applications. • ***CIS Group*** is ISO 27001 certified.
Personnel and Security Awareness Management	***Personnel and Security Awareness Management*** • Security verifications are embedded in HR processes throughout the employment lifecycle, including disciplinary actions tied to security compliance. • All users must annually complete security training and sign key policies such as Acceptable Use and Teleworking Security Standard. Compliance is monitored and enforced.
Access Management	***Access Management (Logical and Physical)*** • Access to data in ***CIS Group***'s environment is granted based on roles (RBAC) and the need-to-know principle. • A strong password policy is enforced and single sign-on and multifactor authentication are enabled wherever possible. • Strong physical access controls are in place at ***CIS Group*** head office. • User access onboarding, maintenance, review and offboarding procedures are in place and regularly audited.
Security Operations	***Endpoint controls*** • An Endpoint Detection Response solution is deployed on all endpoints. • Workstations have FDE (Full Disk Encryption) enabled. • Remote connections must go through the corporate VPN. ***Threat and Vulnerability Management*** • A vulnerability management process is in place to assess threats or vulnerability severity levels and apply corrective actions (patch management). ***Event Monitoring and SOC*** • Security events are logged for users and administrators. • A SOC is in place to monitor and triage log events and notify the security team in case of potential security incidents.

Category	Controls
Communications Security	***Communications and Device Security*** • The network is adequately segregated, and the perimeter is protected by the latest generation technology (e.g., advance email protection, secure web gateway, VPN, MFA, etc.). • Web filtering is in place.
Information Systems Management	***Change Management*** • All changes in the environment are tracked, approved, and controlled through a documented process. ***Capacity Management*** • Capacity is monitored and measures are taken to ensure sufficient resources are available. ***Software Development*** • Access to source code is segregated by business unit. • Secure coding standards are followed throughout the development process. • Tests are performed in isolated environments before deployment to production. • Access to test data is restricted.
Security Incident Management	***Security Incident Management*** • ***CIS Group*** has a documented and operationalized security incident response plan with defined and assigned roles and responsibilities, as well as a breach notification process. • The security incident response plan is tested regularly.
ICT Continuity Management	***ICT Continuity Management*** • Client environments are backed up in Azure. Corporate servers are backed up on premise with an offsite replication. • Controls and monitoring are in place to ensure ICT continuity during adverse events. Recovery procedures have been identified and documented.