Cybersecurity

The ODP Corporation is committed to creating and maintaining high standards of cybersecurity. We have a comprehensive approach to cybersecurity and risk mitigation that includes vigorous protection of customer personally identifiable information (PII) and company confidential information.

The foundation of our cybersecurity program aligns with the internationally-recognized **ISO/IEC 27001** industry security standard. We deploy a multifaceted, in-depth data security defense program that is led by our Chief Information Security Officer and implemented by a team of trained cybersecurity professionals to address data security risks, vulnerabilities, and to protect all company assets. Through people, process, and technology, The ODP Corporation works to identify risks and apply risk mitigation and treatment to each risk based on defined policies and procedures.

The ODP Corporation has information security and privacy policies in place that are informed by regulatory requirements. These policies are reviewed periodically for alignment with current state and federal laws and regulations. We also comply with applicable industry security standards, including the Payment Card Industry Data Security Standard (PCI DSS).

Our technology systems and security program are subject to regular audits by our Internal Audit Team and independent external auditors. Cybersecurity updates are provided to the Board of Directors through quarterly updates to the Audit Committee.

The ODP Corporation maintains a comprehensive, global training and cybersecurity awareness program designed to equip our workforce with relevant information on cybersecurity topics and Company policies. This program fosters a security-conscious workforce by empowering our associates to incorporate security considerations into their everyday duties and make well-informed computing decisions.

The ODP Corporation has a comprehensive approach to cybersecurity and risk mitigation.

SECURITY PROGRAM INCLUDES

- ✓ Multifactor authentication protocols
- ✓ Antivirus/anti-malware software
- ✓ Security operations center
- ✓ Internal/external penetration tests
- ✓ Periodic risk assessments
- ✓ Phishing simulations
- ✓ Bug bounty program
- ✓ Firewalls