Cybersecurity

The ODP Corporation aims for the highest standards of cybersecurity, covering robust protection for our customers' personally identifiable information (PII) and proprietary company data. We have a comprehensive approach to cybersecurity and risk mitigation that is built upon industry-leading standards and specifically aligns with the internationally recognized **ISO/IEC 27001** security framework.

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 cybersecurity risks, vulnerabilities, and to protect the Company's data assets. Through people, process, and technology, The ODP Corporation works to identify risks and apply risk mitigation and treatment to each risk in concert with the Company's policies and procedures.

Our cybersecurity and privacy policies are frequently updated to reflect evolving regulatory requirements, and current state and federal laws. In addition, we adhere to key industry security standards, including the Payment Card Industry Data Security Standard (PCI DSS), to effectuate compliance in all required areas.

Additional oversight is provided through regular audits of our technology systems and cybersecurity programs to enhance our efforts to meet the vast array of ever-evolving compliance standards in our industry. Our Board of Directors is kept informed regarding our cybersecurity measures, mitigation efforts, and the comprehensive cybersecurity program.

To cultivate a security-aware culture, The ODP Corporation has implemented a comprehensive, global training and cybersecurity awareness program. This initiative empowers our associates with essential cybersecurity knowledge, enabling them to integrate security best practices into their daily tasks and make informed security decisions in a computing environment.

Our approach:

- ✓ **Multifactor authentication protocols**
- ✓ **Antivirus/anti-malware software**
- ✓ **Security operations center**
- ✓ **Internal/external penetration tests**
- ✓ **Periodic risk assessments**
- ✓ **Phishing simulations/regular training**
- ✓ **Data encryption**
- ✓ **Bug bounty program**
- ✓ **Firewalls**
- ✓ **Endpoint protection**
- ✓ **Written policies and standards**