At Univar Solutions we understand that our stakeholders seek increasing transparency in relation to Information Security and the measures we are taking to protect ourselves, as well as the individuals and businesses with whom we transact. We seek to provide this information, but in a way that does not compromise our tactics, some of which depend upon confidentiality for optimized efficacy.

Identifying and Mitigating Information Security Risks

We have deployed Firewalls, Application Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and IP/URL filtering to monitor all network traffic flowing between the Internet and the enterprise network. These systems have alerting capability to notify IT personnel when critical events are detected.

Automated vulnerabilities scans are performed across the network on a regular basis. The solutions used to perform the vulnerabilities scans are updated frequently to ensure the latest threats are identified. Any weakness found by the vulnerability scan is assessed to determine risk, priority, and mitigation actions.

There are standard operating systems deployed across the enterprise that include security hardening. All workstations and servers are configured with malware protection programs that are updated on a frequent basis. Workstations have an additional layer of protection that monitors for malicious behavior and Virtual Private Networks (VPNs) are used for remote users when not on a Company network.

An Identity Management System, including Multi Factor Authentication (MFA), is used to manage user account lifecycle and all access requires approval. All passwords must meet a minimum requirement with additional complexity required for privileged accounts. Further, extra authorizations, monitoring and alerts are used in relation to privileged accounts.

In addition, the company does maintain an information security risk insurance policy.

Governance

The Audit Committee of our Board of Directors exercises oversight in relation to our information security matters. On at least a bi-annual basis they review the results of our assessments (some of which are conducted by external consultants). The full Board of Directors exercises oversight in relation to the company’s enterprise risks, which often include risks related to cybersecurity and information security.

On a monthly basis our company’s Risk Steering Committee (which is composed of a cross-section of senior executives) reviews a comprehensive threat metric report that includes reports on endpoint threats, firewall threats, blocked security web requests, and email threat activity including a variety of phishing metrics and reports.

External Audits and Certifications

On an annual basis the company utilizes one or more Red Team/Blue Team, or Purple Team assessments in addition to traditional penetration tests to assess and develop the effectiveness of our security programs. These assessments are designed to provide real-world, practical insight into the strengths and weaknesses of our programs so we can augment and enhance them as appropriate. On an every-other-year basis the company retains an external auditor to assess the company’s programs against the NIST cybersecurity framework.

Training

Every company employee and some contractors are required to undergo various forms of information security training. These training programs range from phishing awareness to the appropriate storage, handling, and accessing of electronic data.