POLICY SCOPE:

Manufacturers worldwide are being targeted by cybercriminals at an astonishing and increasing rate. The rise in cyber-attacks is particularly concerning given that they're occurring during periods of entrenched supply chain bottlenecks. At the same time, manufacturers are experiencing increased vulnerabilities to their businesses due to weaknesses in their supplier networks. Building cyber security protection through an informational infrastructure is essential to agility and resilience for any supply chain organization in today's global marketplace.

TOPIC BACKGROUND:

Cyber Attacks on the manufacturing industry has been triggered by converging and intensifying factors. Vulnerabilities have deepened during the pandemic as hybrid workforces, remote work, and the sudden need to create a "no-touch" work environment have accelerated the deployment of digital solutions, including cloud technologies, client portals and mobile and web-based apps, all of which need to be properly monitored and maintained. Additionally, there are the persistent challenges of creating and monitoring rigorous cybersecurity programs and protocols at numerous locations, as well as supply base third-party networks.

VETERANS TRADING COMPANY POLICY STATEMENT:

The security of the organization's Information technology systems has been identified by Veterans Trading Company's management as a critical business element that requires full management support. Our mission is to develop, implement and maintain an industry best practice Cyber Information and Security Program, integrating established NIST 800-171 controls seamlessly throughout organizational processes. Allowing our supply chain partners and customers stability and reassurance while conducting business transactions with our organization.

	Leadership Commitment Infrastructure Dedicated Resources Responsible Personnel Adequate 3rd Party Contracted Support Adequate Equipment
	Cyber Security Manual Cyber Security Program Overview Element Policies/Procedures Associated Supporting Documents Data Collection Methods and Reporting Record Retention
	Information Systems User Access and Security Information Systems 3rd Party Contractors Oversite and Deliverables Information Systems 3rd Party Licensed Applications (Setting, Management, Audit and Reporting) Information Systems Hardware and Support (Setting, Management, Audit and Reporting) Shared Customer/Supplier and Internal Information Security
	Cyber Security Risk Assessment and Report Breach Response Plan by Type Identify Response Team Utilize 6 Steps Problem Resolution Methodology and PDCA Cycle Communication Plan, Distribution List, Timing
	Cyber Security Personnel Position Descriptions and Job Responsibilities Onboarding Cyber Security Training Requirements Annual Cyber Security Employee Training Requirements Employee Participation Threat Assessment Applications Employee Participation Threat Assessment Audits

DOCUMENT HISTORY

REV	DESCRIPTION OF CHANGE	DATE	CHANGED BY
A	Initial Release	2023-04-25	Scott Toone