	Supplier Cybersecurity Policy		Revision: 0
	Rev. 0	NAC - Corporate Document Number: NAC-100000-PP-POL-000-0003	Houston, TX Date: 26JUL2021

SUPPLIER CYBERSECURITY POLICY

Purpose and Scope


Cybersecurity is an enterprise-wide risk management issue. This Policy describes Nacero's cybersecurity requirements for Suppliers and all parties who access, process, hold or transmit Nacero information.

References

The National Institute of Standards and Technology (NIST) has developed a framework for managing cybersecurity risks. The International Standards Organization (ISO) provides a useful and international standard for cybersecurity programs (ISO 27001).

Requirements

1. Supplier shall safeguard the confidentiality, availability and integrity of Nacero's information by applying current industry best practices in all communications and documentation regarding the materials, equipment and services it supplies and proposes to supply to Nacero. Supplier shall require all of its users handling Nacero information to use strong passwords and two-factor authentication for software programs, platforms and portals that access, store or transmit Nacero information. VPNs (Virtual Private Networks) must be used when accessing or transmitting Nacero information over WiFi.
2. Supplier is responsible for maintaining compliance with relevant regulations and all applicable laws in its dealings with Nacero.
3. Upon request of Nacero, Supplier shall provide full documentation of its own policies and procedures related to how it protects Nacero information.
4. Supplier shall maintain adequate IT business continuity and disaster recovery controls and shall test such controls regularly to ensure effectiveness. Supplier shall promptly disclose all known cybersecurity vulnerabilities that may affect Nacero and reasonably cooperate with Nacero's investigation of any potential cybersecurity vulnerability.
5. Supplier is responsible to prevent all unauthorized access to Nacero information, prevent the misuse of Nacero information, and to promptly detect and rectify any security breaches of Nacero information. Supplier shall notify their Nacero point of contact within six (6) hours of any actual or attempted breach of Supplier's network or Nacero information, take all appropriate corrective action solely at its expense, and provide a detailed root cause analysis report to Nacero within five (5) days. Remediation plans, including identification of any Nacero data losses or alteration and verification of any software and patch integrity and authenticity must be submitted for Nacero's written approval within fourteen (14) days, with corrective actions implemented within ninety (90) days or other mutually agreed time period.
6. Supplier shall designate an individual responsible for its internal management of cybersecurity, shall identify such individual in all contracts with Nacero and shall give Nacero written notice of such person's replacement in such case.
7. Nacero retains the right to periodically audit Supplier's and Supplier's affiliates operations, processes, systems, and documents that are related to Supplier's compliance with this Policy. Supplier agrees to promptly implement all recommendations arising from any such audit.
8. Nacero reserves the right to terminate its relationship with Supplier based on Supplier's non-compliance with this Policy.
9. Nacero reserves the right to update or modify this Policy from time to time by posting the latest version on its website.

	Supplier Cybersecurity Policy		Revision: 0
	Rev. 0	NAC - Corporate Document Number: NAC-100000-PP-POL-000-0003	Houston, TX Date: 26JUL2021

Indemnity

Supplier shall indemnify, defend and hold harmless Nacero, its affiliates, employees, agents and other contractors and suppliers against all and any actions, costs, claims, damages, losses, expenses and liabilities of whatever kind made relating to or arising out of the breach by Supplier of the terms of this Policy.

Reference Documents

Document Number	Document Title	Section
NAC-100000-FI-POL-000-0001	Delegation of Authority Matrix	All
NAC-100000-PP-POL-000-0003	Supplier Cybersecurity Policy	All
NAC-100000-IT-POL-000-0001	Cybersecurity Response Plan	All
NAC-100000-PP-STD-000-0002	Company Card Procedure	All
NAC-100000-LE-AGM-000-0003	Nondisclosure Agreement	All
NAC-100000-PP-POL-000-0009	Travel and Entertainment Policy	All