

# PRODUCT CYBERSECURITY

---

- A. SUMMARY
- B. APPLICABILITY
- C. DEFINITIONS
- D. PRINCIPLES
- E. POLICY

---

PRINTED COPIES OF THIS DOCUMENT ARE UNCONTROLLED - PLEASE VERIFY CURRENT ISSUE BEFORE USE



## **A. SUMMARY**

This Carrier Product Cybersecurity Policy provides guidelines and instructions for key practices and activities. These guidelines help Product, Solutions and Services development teams deliver safe, reliable, and competitive Products, solutions and Services securely.

## **B. APPLICABILITY**

This Policy applies to Carrier and any Product or Service, as defined in [Exhibit 1](#). Carrier will ensure that its Service Providers comply with this Policy or equivalent requirements through appropriate contractual agreements. Local laws, regulations, and other restrictions applicable to Carrier or any Operating Business will be applied if they conflict with this Policy.

The CTO, SVP of Global Engineering is the executive sponsor of this policy. They designate the Carrier Chief Product Security Officer (CPSO) as the owner responsible for maintaining, fulfilling, and enforcing the provisions of this Policy. Any deviation from this Policy must be approved in writing by the Carrier CPSO (or designee) before implementation.

## **C. DEFINITIONS**

Exhibit 1 provides definitions for terms used in this Policy.

All capitalized terms not defined in this Policy (including Exhibit 1) are defined in [CPM 1: Governance and Definitions](#) including [Exhibit 1: Compliance Glossary](#)



**CORPORATE POLICY MANUAL**

**D. PRINCIPLES**

Carrier will follow these Product Cybersecurity principles in all products, service, and solutions activities for external to Carrier distribution and/or revenue:

1. **Secure Development:** Applying the Carrier Way is essential for secure product development and support.
2. **Team Effort:** Cybersecurity is everyone's responsibility and requires teamwork, awareness, expertise, collaboration, transparency, and continuous improvement.
3. **Security Controls:** Implementing proactive and reactive security measures throughout the product lifecycle is necessary to ensure success.
4. **Risk Management:** Identifying and managing cybersecurity risks in an auditable way is crucial for maintaining security standards.
5. **High Standards:** Continuously improving capabilities in secure deployment, threat intelligence, monitoring, and incident response is required to provide excellent support and transparency.
6. **Best Practices:** Aligning with and exceeding industry best practices to innovate and differentiate Carrier's brand and offerings.

---

**PRINTED COPIES OF THIS DOCUMENT ARE UNCONTROLLED - PLEASE VERIFY CURRENT ISSUE BEFORE USE**

Last updated December 2024 – © Carrier 2024. All Rights Reserved



## CORPORATE POLICY MANUAL

### E. POLICY

1. **Compliance with Law:** At a minimum, Carrier will comply with all laws and regulations relating to Cybersecurity applicable to its Operating Businesses worldwide. Carrier will comply with all applicable cybersecurity laws and regulations worldwide.
2. **General:** All external releases must evidence compliance with GPC process and have remediation plans for all released vulnerabilities.
3. **Codes and Standards:** Carrier will adhere to industry codes and standards to maintain competitive advantage and comply with regulations. The CPSO (or designee) will establish strategies and identify relevant standards.
4. **Product Cybersecurity Standards:** The CPSO (or designee) will create and update cybersecurity standards and procedures for product development and support. These standards will ensure risk management, compliance, and optimal results
5. **Risk Management:** Responsible parties will work with the CPSO (or designee) to identify and manage cybersecurity risks using a common methodology. Risks will be scored and managed according to established tolerance levels.
6. **Governance:** All product and service changes must comply with industry standards and include cybersecurity controls. Independent gating and release approvals are required before deployment.
7. **Cybersecurity Tooling:** Cybersecurity tools will be standardized and centrally managed by Carrier Global Product Cybersecurity (GPC) to ensure consistent execution and compliance.
8. **Cybersecurity Testing:** Testing will be independent, standardized, and managed by GPC. Regular internal and external testing will ensure compliance and mission success
9. **Deliverables:** Cybersecurity artifacts will be collected throughout all development phases and retained according to Carrier's policies. This ensures auditability and continual improvement.
10. **Enforcement:** Non-compliance with this Policy may result in disciplinary action. Carrier will maintain fair and consistent disciplinary procedures across the enterprise.

---

PRINTED COPIES OF THIS DOCUMENT ARE UNCONTROLLED - PLEASE VERIFY CURRENT ISSUE BEFORE USE