Linx Statement on the Cyber Resilience Act for Customers

Purpose

This statement explains how Linx approaches the EU Cyber Resilience Act (CRA) for products with digital elements and what customers can expect from Linx in relation to product cybersecurity, vulnerability handling, and security communications.

Linx is committed to improving the cybersecurity of its products and supporting customers with a controlled, documented approach to vulnerability management. Our product security processes are designed to help identify, assess, remediate, communicate, and retain evidence for cybersecurity vulnerabilities and product cybersecurity incidents affecting Linx products, related software, firmware, cloud services, applications, and relevant third-party components used within those products.

Linx welcomes reports of potential cybersecurity vulnerabilities affecting our products and services and assesses them through our Product Security Incident Response Team (PSIRT).

Our commitment to customers

Linx recognises that customers need confidence that product cybersecurity is being managed throughout the product lifecycle. In support of this, Linx maintains product security governance intended to support CRA readiness and responsible vulnerability handling.

- We maintain a Product Security Incident Response Team (PSIRT) to receive, assess, coordinate, and track product cybersecurity vulnerabilities and incidents.
- We accept vulnerability reports from customers, security researchers, suppliers, internal teams, and monitoring sources.
- We assess reported issues for validity, product relevance, customer exposure, exploitability, severity, and potential regulatory implications.
- We coordinate remediation, mitigation, validation, and customer communication where action is required.
- We retain records and evidence of decisions, investigations, communications, and outcomes.

How to report a concern

Customers, researchers, and partners can report potential cybersecurity vulnerabilities to security@linxglobal.com including: product name, version, technical detail, reproduction steps, and observed impact to help Linx investigate more effectively.

Linx Printing Technologies Ltd, Linx House, 8 Stocks Bridge Way, Compass Point Business Park, St Ives, Cambridgeshire PE27 5JL, United Kingdom
T +44 (0)1480 302100 **F** +44 (0)1480 302116 **E** sales@linxglobal.com

www.linxglobal.com

Registered in England No. 2066629

What customers can expect from Linx

Area	What customers can expect
Reporting channel	A defined route for reporting product cybersecurity concerns via security@linxglobal.com.
Assessment	A structured review of product relevance, impact, severity, exposure, and potential regulatory implications.
Coordination	PSIRT-led coordination across product security, engineering, product management, and legal/compliance as required.
Remediation	Consideration of fixes, mitigations, workarounds, supplier actions, or formal risk treatment.
Communication	Customer-facing information where action, awareness, or product status clarification is needed.
Evidence	Documented records of decisions, assessments, communications, and closure outcomes.

Information customers should include in a report

To help Linx investigate quickly and accurately, customers should provide as much of the following as possible:

- Product name and model
- Software or firmware version
- Configuration or deployment context
- Detailed technical description
- Reproduction steps
- Observed impact
- Any evidence of exploitation or attempted abuse
- Supporting logs, screenshots, captures, or files where appropriate

Linx Printing Technologies Ltd, Linx House, 8 Stocks Bridge Way, Compass Point Business Park, St Ives, Cambridgeshire PE27 5JL, United Kingdom
T +44 (0)1480 302100 **F** +44 (0)1480 302116 **E** sales@linxglobal.com

www.linxglobal.com

Registered in England No. 2066629

Frequently asked questions:

Does Linx accept reports from security researchers?

Yes. Linx supports responsible coordinated disclosure and accepts reports from researchers, customers, suppliers, and internal teams.

Will every reported issue result in a software update?

No. The response depends on validation outcome, severity, exploitability, product lifecycle status, and technical feasibility. In some cases, mitigation or guidance may be the appropriate response. The nature and availability of any remediation may depend on product lifecycle status, technical feasibility, customer configuration, and applicable support arrangements.

How does Linx handle supplier vulnerabilities?

Supplier vulnerabilities that may affect a Linx product are assessed through the PSIRT process, including dependency review, exposure analysis, remediation planning, and communication decisions.

Does Linx keep records of vulnerability decisions?

Yes. Linx maintains auditable PSIRT records covering intake, assessment, evidence, remediation, communications, and closure.

Contact

For product cybersecurity reports or questions related to vulnerability disclosure, contact security_@linxglobal.com.

This statement is provided for general information purposes only and describes Linx's current approach to product cybersecurity and vulnerability management. It does not create any contractual obligations, warranties, service levels, or commitments and does not amend or supersede any agreement between Linx and its customers. Product-specific obligations, support commitments, and customer rights are governed solely by the applicable contractual documentation.

This statement applies only to Linx products, software, firmware, cloud services, and applications that are commercially supported by Linx. Certain products, legacy products, end-of-life products, third-party products, or customer-modified solutions may be subject to different security, support, or maintenance arrangements.

Linx Printing Technologies Ltd, Linx House, 8 Stocks Bridge Way, Compass Point Business Park, St Ives, Cambridgeshire PE27 5JL, United Kingdom
T +44 (0)1480 302100 **F** +44 (0)1480 302116 **E** sales@linxglobal.com

www.linxglobal.com

Registered in England No. 2066629