

VIRTUAL CODE · NETWORK CATALOGUE PUBLICATION

Cyber Incident & Resilience Act

Issuing office: Meridian Cyber Defense Command

An incident record distinguishes observations, assumptions and recommended corrections.

Network scope and limits

United Network Federation is an independently presented, privately administered digital-network governance framework. Its charter, participation rules, registry entries, reviews and dispute procedures operate only within services and among participants that adopt them. These publications are not government instruments, statutory licenses, judicial orders, public registrations or proof of independent security certification. A registry match confirms a publication in this network catalogue only. Sponsorships or external approvals require separate, verifiable evidence.

Record particulars

Document identifier	UNC-140
Record category	Virtual Code
Issuing institution	Meridian Cyber Defense Command
Subject / named party	UNF virtual institutions
Catalogue publication date	2026-10-07
Registry listing status	PUBLISHED IN NETWORK CATALOGUE
Validity and limitation	Valid only as a network-specific network catalogue record. Review date: 2027-10-07; not a government or statutory document.
§ 140.1 · Purpose and virtual scope	This network-defined Code governs sample cyber incidents within the UNF universe only. It has no effect in any real jurisdiction.
§ 140.2 · Defined terms	“Institution” means an expressly network-defined UNF body. “Record” means a published sample network catalogue entry. “Review” means a documented scenario process concerning sample cyber incidents.
§ 140.3 · Responsible institution	Meridian Cyber Defense Command coordinates this Code, with procedural support from VDJA and oversight from OFIG.
§ 140.10 · Primary rule	An incident record distinguishes observations, assumptions and recommended corrections.
§ 140.11 · Implementation duties	A scenario incident report must identify impact, containment boundaries, recovery steps and unresolved findings. Reassessment checks corrective evidence rather than relying on a declaration.

§ 140.12 · Protected principle	Each application must respect containment and recovery learning. The institution records the purpose, evidence limits, response opportunity and responsible reviewer.
§ 140.13 · Limitations	No action under this network-defined Code permits real-world surveillance, access to accounts, seizure, enforcement, licensing or legal determination.
§ 140.20 · Notice and record	Before an adverse network-defined determination, the responsible office states the facts and cites UNC-140 § 140.10, allowing at least fourteen scenario days for a response.
§ 140.21 · Outcome and appeal	A reasoned outcome states findings, uncertainties and corrective options. Review follows UNC-240; tribunal proceedings also observe UNC-100.
§ 140.22 · Publication and retention	Sample public records include a network-scope notice, issuer, status, date and related record identifiers. Private portal submissions remain separate and are subject to thirty-day receipt expiry and removal on a later report-service request.
§ 140.30 · Review cycle	The coordinating institution reviews this network-defined Code annually and publishes a change note. Material amendments require consultation and recorded approval within the story.
§ 140.31 · Effective date and transition	Version 1.0 takes effect on 7 October 2026 in the network-defined chronology. Earlier sample matters retain their published procedural safeguards.

Review, corrections and verification

Record amendments may be published with a version history, responsible issuing office and reason for change. Verify the exact identifier in the federation registry. A catalogue match verifies published data and file integrity only, not third-party approval or statutory authority.

Cross-references: UNF-CHARTER-001, UNC-100

Record edition

Network publication edition 3.0. No external government, commercial, judicial, sponsor or certification claim is independently verified by this publication.