CYBERGLASS SECURITY STANDARDS

Post-Quantum Cryptography and Cryptographic Agility Standard

Requirements for [Company Name]'s move to NIST post-quantum algorithms (ML-KEM, ML-DSA, SLH-DSA), protection against harvest-now-decrypt-later, and cryptographic agility across systems, suppliers and AI pipelines.

Organization	[Company Name]
Document ID	STD-05
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

FREE SAMPLE

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Start with the inventory (section 5) and prioritization (section 6); you cannot plan migration without knowing where cryptography is used.
- Confirm the current versions of NIST IR 8547 and any national rules that apply to you before approving the dates in section 7.
- Send the section 10 supplier requirements to your critical vendors early; much of your cryptography sits in their products.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Free sample from STD-05. Full editable standard at cyberglass.ai/post-quantum-cryptography.html

1. Purpose

This Standard sets [Company Name]'s requirements for moving from public-key cryptography that a large quantum computer could break (RSA, elliptic-curve and classical Diffie-Hellman) to the post-quantum cryptography (PQC) algorithms standardized by NIST, and for building cryptographic agility so future changes are faster. It is aligned with NIST IR 8547, Transition to Post-Quantum Cryptography Standards (final, October 2026), which deprecates quantum-vulnerable public-key algorithms after 2030 and disallows them after 2035.

The most urgent risk is **harvest now, decrypt later**: attackers can record encrypted traffic or copy encrypted data today and decrypt it once a capable quantum computer exists. Data that must stay confidential for many years is already exposed if it travels or is stored under quantum-vulnerable key exchange.

What post-quantum cryptography is

Post-quantum cryptography (PQC) means new public-key algorithms that are designed to stay secure even against attackers who have a large, error-corrected quantum computer. They run on today's ordinary computers, phones, servers and security hardware; no quantum equipment is needed to use them.

Why it is needed	Most of today's public-key cryptography (RSA, elliptic-curve and classical Diffie-Hellman) relies on maths problems that a large quantum computer could solve quickly using Shor's algorithm. Such a computer does not exist yet, but data recorded today could be decrypted when one does.
What it does	PQC replaces those algorithms in two jobs: **key establishment**, agreeing secret keys to encrypt connections and data (ML-KEM, FIPS 203), and **digital signatures**, proving who sent something and that it was not changed: certificates, code, firmware and documents (ML-DSA, FIPS 204; SLH-DSA, FIPS 205).
What stays the same	Symmetric encryption (AES) and hash functions (SHA-2, SHA-3) remain secure at current sizes; AES-256 is preferred for long-lived data. Protocols such as TLS, VPNs and PKI keep working, using new algorithms inside them.
What changes in practice	Keys, ciphertexts and signatures are larger, so some systems, devices and networks need upgrades or tuning. Certificates, signing systems, hardware security modules and supplier products all need new versions.
What it is not	PQC is not quantum key distribution (QKD), which uses special quantum hardware and links; NIST and most national authorities recommend PQC rather than QKD for general use. It is also not a product you buy once: it is a migration across every system that uses public-key cryptography.

FREE SAMPLE

2. Objectives

The objectives of this Standard are to:

a) know where and how cryptography is used across [Company Name], including in products and services from suppliers

b) protect long-lived confidential data first, by moving key establishment for high-risk data flows to hybrid or post-quantum methods

c) complete migration of key establishment for high-value systems by 31 December 2030 and of digital signatures by 31 December 2031

d) stop using quantum-vulnerable public-key algorithms entirely by 31 December 2035

e) make cryptography replaceable through configuration rather than code changes, so future algorithm changes take months, not years

Free sample from STD-05. Full editable standard at cyberglass.ai/post-quantum-cryptography.html

Reference	Relevance
NIST SP 800-227 (September 2025)	Recommendations for key encapsulation mechanisms, including hybrid combiners
NIST SP 800-56C, SP 800-131A, SP 800-208	Key derivation and combiners; algorithm transitions; stateful hash-based signatures
Government of Canada PQC roadmap (ITSM.40.001, 2025)	Federal plans from April 2026; high-priority systems by end of 2031; all by end of 2035
UK NCSC PQC migration timelines (2025)	Discovery and plan by 2028; priority migrations by 2031; complete by 2035
EU coordinated PQC roadmap (2025)	Start by end of 2026; high-risk use cases by end of 2030
STD-04, AI-04, IT-04	AI agent credentials, AI vendor assessment, information security policy

Appendix A. Regulatory and Government Timelines

Dates below summarize public guidance as of November 2026 for planning. Check the current versions of NIST IR 8547, NIST SP 800-131A and any rules that apply to you; this is not legal advice.

Jurisdiction	Source	Key dates
United States	NIST IR 8547; FIPS 203–205 (Aug 2024); NSA CNSA 2.0; EO 14412 and OMB M-26-15 (federal)	Aug 2024: FIPS 203, 204, 205 published; 1 Jan 2027: new national security system acquisitions must support CNSA 2.0 unless excepted; 31 Dec 2030: federal high-value systems PQC key establishment; 31 Dec 2031: signatures; further CNSA 2.0 milestones to 2033; after 2030 quantum-vulnerable algorithms deprecated and after 2035 disallowed (NIST IR 8547)
Canada	Cyber Centre roadmap ITSM.40.001 (June 2025) and Treasury Board direction (federal)	Apr 2026: initial departmental migration plans and annual progress reports; Apr 2027: updated plans with cryptographic discovery; Apr 2028: transition begins; end 2031: high-priority systems complete; end 2035: all remaining systems, with legacy algorithms removed
United Kingdom	NCSC guidance	Discovery and plan by 2028; highest-priority migrations by 2031; complete by 2035
European Union	NIS Cooperation Group coordinated roadmap	Start by end of 2026; high-risk use cases by end of 2030; as much as feasible by 2035
Australia	ASD guidance	Refined plan by end of 2026; transition started by end of 2028; complete by end of 2030

FREE SAMPLE

Free sample from STD-05 · Full editable standard at cyberglass.ai/post-quantum-cryptography.html