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

PREVIEW

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.

Preview pages · full editable Word file at cyberglass.ai/shop

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.

PREVIEW

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

Preview pages · full editable Word file at cyberglass.ai/shop

3. Scope

This Standard applies to:

a) all systems, applications, infrastructure, devices and cloud services that create, protect, transmit or verify [Company Name] or client data

b) all uses of public-key cryptography: TLS and VPNs, SSH, email security, certificates and PKI, code and document signing, identity federation and tokens, encrypted backups and key management

c) AI pipelines and agents: connections between agents, tools, model services and data stores; signing of models, datasets and software; encryption of training data, embeddings and logs

d) hardware security modules (HSMs), smart cards, security keys and embedded or operational technology devices

e) suppliers and their products and services that handle [Company Name] or client data

4. Approved Algorithms

CONTROL ID **STD-05-4**
Maps to NIST CSF 2.0: PR.DS-01, PR.DS-02
Maps to ISO/IEC 27001:2022: A.8.24
Maps to NIST SP 800-53 Rev. 5: SC-12, SC-13

Purpose	Approved for new deployments	Default	Notes
Key establishment (KEM)	ML-KEM (FIPS 203); hybrid ML-KEM with ECDH during transition	ML-KEM-768 (ML-KEM-1024 for long-lived Restricted data)	HQC is being standardized by NIST as a backup KEM
Digital signatures (general)	ML-DSA (FIPS 204)	ML-DSA-65	FN-DSA (FIPS 206, in development) may suit size-constrained uses once published
Signatures for long-lived roots and firmware	SLH-DSA (FIPS 205); stateful hash-based LMS or XMSS (SP 800-208) where key state can be managed reliably	SLH-DSA for root and firmware signing keys	Larger signatures; plan storage and bandwidth
Symmetric encryption	AES-128, AES-192, AES-256	AES-256 for Restricted and long-lived data	Not materially weakened by known quantum attacks at these key sizes
Hashing and MACs	SHA-2 (SHA-256 and above), SHA-3, HMAC, KMAC	SHA-256 or SHA-384	SHA-1 is not approved for signatures

Quantum-vulnerable (to be replaced)	Status under NIST IR 8547	[Company Name] rule
RSA (signatures and key transport)	Deprecated after 2030; disallowed after 2035	No new uses after [Month 12] without an exception
ECDSA and EdDSA signatures	Deprecated after 2030; disallowed after 2035	Migrate by 31 December 2031

PREVIEW

Preview pages · full editable Word file at cyberglass.ai/shop

Situation	Action
Archive encrypted with symmetric keys that are themselves wrapped with RSA or elliptic-curve keys (common in backup and file encryption tools)	Re-wrap the data keys under a symmetric or PQC key-encryption key; full re-encryption of the data is usually not needed
Files or emails encrypted directly to RSA or elliptic-curve public keys (for example older email or file encryption)	Re-encrypt if the data must stay confidential beyond 2030; otherwise isolate access and shorten retention
Data that has passed its retention period	Delete it; deleted data cannot be decrypted later
Data that was sent in the past over classical TLS or VPN	Cannot be protected retroactively; assume recorded copies could be decrypted in future, and factor this into risk assessments and client commitments

7. Migration Phases and Milestones

CONTROL ID **STD-05-7**
Maps to NIST CSF 2.0: ID.RA-06, GV.RM-04
Maps to ISO/IEC 27001:2022: cl. 6.1.3, A.8.24
Maps to NIST SP 800-53 Rev. 5: PM-9, SC-13

PREVIEW

Phase	Target	Required outcomes
1 Inventory and plan	[Month 6], at latest [mid-2027]	Cryptographic inventory complete for priority 1–2 systems; owners named; migration plan and budget approved; supplier questions sent
2 Hybrid for high-risk flows	2026–2028	Hybrid ML-KEM key establishment on internet-facing services, VPNs and third-party links carrying long-lived confidential data; PQC-capable HSMs and libraries selected
Supplier attestations	[1 January 2028]	Critical suppliers have attested PQC algorithm support and delivered dated roadmaps (section 10)
AI data transport	[End of 2028]	Vector stores, embedding services and model weights moved to hybrid ML-KEM-768 transport (section 12)
3a Key establishment	31 December 2030	PQC or hybrid key establishment for all high-value and sensitive systems; TLS 1.3 everywhere it is supported
3b Signatures	31 December 2031	PQC signatures for code signing, firmware, PKI roots and issuing CAs, identity tokens and document signing for high-value systems
4 Disallow classical	31 December 2035	No use of RSA, ECDSA, EdDSA, DH or ECDH anywhere; legacy algorithms disabled, not just supplemented

The 2030 and 2031 targets match US federal deadlines for high-value systems (Executive Order 14412 and OMB Memorandum M-26-15) and fit within NIST IR 8547's deprecation after 2030. Organizations with less exposure may set later internal dates for low-priority systems, but not later than 2035.

Preview pages · full editable Word file at cyberglass.ai/shop