NIS2 COMPLIANCE GAP ANALYSIS

VeriPulse B.V.

Date: April 2026

Frameworks Referenced

EU Directive 2022/2555 (NIS2) | Cyberbeveiligingswet (Cbw) Draft | NCSC-NL Guidance

Prepared by: Haitam Laafar

Table of Content

1. Executive Summary

1.1 Purpose of This Assessment

This document presents the findings of an internal NIS2 compliance gap analysis conducted for VeriPulse B.V **(fictional).** Its purpose is to determine VeriPulse's current compliance posture against the requirements of EU Directive 2022/2555 (NIS2) and the forthcoming Dutch implementing legislation, the Cyberbeveiligingswet (Cbw), and to provide a prioritised roadmap for achieving compliance before enforcement begins.

1.2 Regulatory Context

The NIS2 Directive is an EU-wide cybersecurity law that entered into force in January 2023, with a Member State transposition deadline of 17 October 2024. It significantly expands the scope of its predecessor (the original NIS Directive) in two ways: more sectors are covered, and the security obligations are substantially more demanding.

In the Netherlands, NIS2 is being transposed via Cyberbeveiligingswet (Cbw). As of April 2026, the Cbw is in its final stages of parliamentary review and is expected to enter into force in Q2–Q3 2026, with a grace period before active enforcement. Despite the legislative delay, the Dutch Ministry of Economic Affairs has advised in-scope organisations to begin compliance preparations immediately. Voluntary registration with the NCSC (National Cyber Security Centre) has been possible since October 2024.

1.3 NIS2 Applicability

VeriPulse B.V. meets the criteria for classification as an Important Entity under NIS2 Annex II on two independent grounds:

- Size: 75 employees exceeds the medium-sized enterprise threshold (50+ employees)
- Turnover: €14M annual turnover exceeds the €10M threshold
- Sector: VeriPulse operates a SaaS platform processing patient-reported health data for hospitals and pharmaceutical clients, placing it within the digital services and health-adjacent sectors covered under NIS2 Annex II

As an Important Entity, VeriPulse is subject to all ten risk-management measures under Article 21 of the Directive, the multi-stage incident reporting obligation (24h / 72h / 30-day), and mandatory registration with the NCSC upon Cbw entry into force.

1.4 Summary of Findings

This assessment identified significant compliance gaps across 8 of the 10 Article 21 requirement areas. No requirement area was found to be fully compliant. The most critical gaps are:

- **No documented Information Security Policy or risk management framework:** The foundational requirement of Article 21(2)(a) is entirely unmet
- **No Incident Response Plan:** VeriPulse has no documented procedure for detecting, escalating, or reporting a significant incident within the legally required 24-hour window
- **No supply chain security controls or third-party risk assessments:** VeriPulse relies on multiple cloud and API service providers with no formal security review process
- **No Business Continuity or Disaster Recovery plan:** a major incident could result in extended service unavailability with no structured response
- Access control and **MFA inconsistently applied**: privileged access to production systems is not governed by a formal policy and MFA is not enforced across all entry points

1.5 Risk of Non-Compliance

Non-compliance with the Cyberbeveiligingswet upon its entry into force carries the following consequences for VeriPulse as an Important Entity:

Consequence	Detail
Administrative fines	Up to **€7,000,000** or **1.4%** of global annual turnover, whichever is higher
Management liability	Board members may be held personally liable for failure to oversee compliance
Supervisory measures	The competent authority may impose binding instructions, audits, or temporary service restrictions
Reputational damage	Hospital and pharma clients have their own regulatory obligations; a **NIS2** enforcement action would trigger immediate contractual and procurement consequences

Beyond regulatory risk, VeriPulse's current security posture presents a genuine operational risk. The combination of sensitive health-adjacent data, immature incident response capability, and undocumented access controls creates a high probability of a significant incident with no documented means of managing it.

2. Company & Scope Definition

2.1 Organisation Profile

Field	Detail
Legal Name	VeriPulse B.V.
Registration	Chamber of Commerce (KvK), Utrecht
Headquarters	Utrecht, Netherlands
Employees	75 (full-time equivalent)
Annual Turnover	€14,000,000
Core Business	SaaS platform for Patient-Reported Outcome **(PRO)** data collection and analytics
Primary Clients	Hospitals, pharmaceutical companies
Data Processed	Patient-reported symptom and outcome data; pseudonymised by default but linkable to patient records held by hospital clients
Cloud Infrastructure	Microsoft Azure (primary); AWS (secondary data processing pipeline)

2.2 Organisational Structure

VeriPulse does not have a dedicated security function. The current security-relevant staffing is:

- **IT Manager:** Responsible for all infrastructure, cloud administration, endpoint management, and vendor relationships.
- **CTO:** Technical oversight, architectural decisions. No documented security governance mandate.
- **Data Protection Officer (DPO):** appointed under GDPR, part-time/external. Focused solely on data privacy.
- **No CISO, Security Analyst, or GRC function exists.**

2.3 NIS2 Classification

Entity Type: Important Entity

Criterion	Threshold	VeriPulse Status
Employees	≥ 50	75 employees
Annual turnover	≥ €10M	€14M
Sector (Annex II)	Digital services / health-adjacent	SaaS platform serving healthcare clients

Note: Should VeriPulse grow beyond 250 employees or €50M turnover, reclassification to Essential Entity status would apply, triggering stricter supervisory obligations.

2.4 Assets In Scope

Asset Category	Examples	Relevance
Cloud infrastructure	Azure tenant, AWS pipeline environment	Primary operational environment
Application layer	VeriPulse SaaS platform, admin portal, API endpoints	Core service delivery
Data assets	Patient-reported outcome datasets, client config data, authentication credentials	Sensitive data processed under GDPR and NIS2
Integration interfaces	API connections to hospital systems	Supply chain / third-party risk surface
Endpoints	Developer laptops (~40), company mobile devices	Access points to production systems
Identity & access systems	Azure Active Directory, VPN, SSH access to servers	Access control perimeter

2.5 Assets Out of Scope

The following are explicitly excluded from this assessment:

- Physical security at Utrecht office premises.
- Personal devices not managed by VeriPulse IT.
- Client-side systems. (hospital platforms)
- Financial systems. (PCI-DSS)

3. Methodology

3.1 Assessment Approach

This gap analysis was conducted using a structured document review and interview-based methodology. The assessment evaluated VeriPulse's current security controls and documentation against each of the ten risk-management measures prescribed by Article 21(2) of the NIS2 Directive.

The assessment was carried out across two phases:

Phase	Activity	Output
Scoping	Reviewed company profile, regulatory applicability, and asset inventory	Scope definition (Section 2)
Analysis & Reporting	Gap scoring, risk assessment, remediation prioritisation	Sections 4–7 of this document

3.2 Evidence Sources

Source	Type	Findings
IT Manager interview	**Interview**	Primary source for current-state controls description
CTO interview	**Interview**	Architectural decisions, third-party service rationale
Azure tenant configuration review	**Technical observation**	Access control, MFA status, logging configuration
Existing documentation review	**Document review**	No formal IS Policy, IRP, or BCP found
Third-party contract review	**Document review**	No security clauses identified in reviewed vendor agreements

3.3 Scoring Framework

Each Article 21 requirement area was assessed and assigned a compliance status using the following three-tier rating:

Rating	Label	Definition
🔴	**Non-Compliant**	No controls exist, or controls are entirely inadequate. Immediate action required.
🟡	**Partially Compliant**	Some controls exist but are undocumented, inconsistently applied, or materially incomplete. Remediation required before enforcement.
🟢	**Compliant**	Controls are documented, implemented, tested, and proportionate to VeriPulse's risk profile.

Each gap finding includes:

- **Current state:** what exists today.
- **Required state:** what NIS2 Article 21 requires.
- **Gap description:** the specific delta between current and required.
- **Risk implication:** consequence of leaving the gap unaddressed.

3.4 Limitations of This Assessment

This assessment was conducted as an internal review and carries the following limitations:

- No penetration testing or technical vulnerability scanning was performed. Technical findings are based on configuration review and interviews, not active testing.

- The Cyberbeveiligingswet had not entered into force at the time of this assessment. Analysis is based on the NIS2 Directive text directly and the Cbw draft bill. Final implementing regulations may introduce additional requirements.

- This assessment does not constitute a legal opinion. VeriPulse should seek qualified legal advice regarding its specific obligations under the Cbw upon enactment.

4. Gap Analysis

4.1 Summary of Findings

#	Requirement Area	Status	Status Label
(a)	Risk Analysis & Information Security Policies	🔴	**Non-Compliant**
(b)	Incident Handling	🔴	**Non-Compliant**
(c)	Business Continuity, Backup & Disaster Recovery	🔴	**Non-Compliant**
(d)	Supply Chain Security	🔴	**Non-Compliant**
(e)	Network & IS Security, Development & Maintenance	🟡	**Partially Compliant**
(f)	Effectiveness Assessment & Cybersecurity Testing	🔴	**Non-Compliant**
(g)	Cyber Hygiene & Security Training	🟡	**Partially Compliant**
(h)	Cryptography & Encryption	🟡	**Partially Compliant**
(i)	HR Security, Access Control & Asset Management	🟡	**Partially Compliant**
(j)	MFA & Secure Communications	🟡	**Partially Compliant**

4.1 Detailed Findings

Requirement (a): Risk Analysis & Information Security Policies	🔴 Non-Compliant
Current State	No Information Security Policy exists. No formal risk management process has been conducted. The IT Manager makes risk-related decisions on an arbitrary basis, with no documented methodology, risk register, or board approval.
Required State	Article 21 (2) (a) requires organisations to have documented policies on information security risk analysis, and to have conducted a formal risk assessment of their network and information systems. Policies must be approved at **board level** and reviewed periodically.
Gap	VeriPulse has no IS Policy and no risk assessment record. There is no documented link between identified risks and any implemented controls. This is the foundational gap as all other Article 21 requirements depend on a functioning risk management framework.
Risk Implication	Without a risk management framework, VeriPulse cannot demonstrate proportionate control selection to a regulator. This gap also means that risks are not being systematically identified or tracked, creating a direct probability of undetected exposure. As the baseline requirement under Article 21, non-compliance here implies structural non-compliance across all other measures.

Requirement (b): Incident Handling	🔴 Non-Compliant
Current State	No Incident Response Plan (IRP) exists. There is no documented procedure for detecting, classifying, escalating, or responding to a cybersecurity incident. There is no defined escalation path, no named incident owner, and no awareness of the NIS2 reporting obligations.
Required State	Article 21(2)(b) requires documented incident handling procedures that cover detection, classification, containment, eradication, recovery, and post-incident review. Article 23 separately requires that significant incidents be reported to the national CSIRT within **24 hours** of detection, with a detailed notification within **72 hours** and a final report within one month.
Gap	VeriPulse has no IRP and no defined reporting chain. Staff are not aware of what constitutes a reportable incident under NIS2, nor of the legal reporting timelines. No contact information for NCSC-NL is documented.
Risk Implication	In the event of a significant incident VeriPulse would be unable to respond in a structured manner and would almost certainly miss the 24-hour early warning deadline. Missing this deadline is itself an independent violation of the Directive.

Requirement (c): Business Continuity, Backup & Disaster Recovery	🔴 Non-Compliant
Current State	No Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) is documented. There is no evidence that backup configurations have been established, nor that **Recovery Time Objectives (RTOs)** or **Recovery Point Objectives (RPOs)** have been defined.
Required State	Article 21(2)(c) requires organisations to have documented plans for business continuity and disaster recovery, including defined **RTOs** and **RPOs**, backup procedures, and evidence that recovery capabilities are tested periodically.
Gap	VeriPulse operates a SaaS platform on which hospital clients depend for patient data collection. No formal continuity plan exists. RTOs and RPOs have not been defined. Backup configurations are untested. There is no documented procedure for communicating with clients during a service disruption.
Risk Implication	A prolonged platform outage with no recovery plan would directly impact hospital operational workflows. Given VeriPulse's contractual obligations to healthcare clients, an unmanaged outage creates both regulatory exposure under NIS2 and significant commercial liability. The absence of tested backups means that data loss in a destructive attack cannot be bounded.

Requirement (d): Supply Chain Security	🔴 Non-Compliant
Current State	VeriPulse relies on multiple third-party service providers including **Microsoft Azure, AWS** and **Atlassian Jira.** No formal security assessment has been conducted on any of these providers.
Required State	Article 21(2)(d) requires organisations to address security risks in supply chains, including the security posture of direct suppliers and service providers. Organisations must assess the cybersecurity practices of their suppliers and ensure that security requirements are reflected in contractual agreements.
Gap	No supplier security assessments exist. No vendor risk register is maintained. Contracts with third-party providers contain no security obligations, incident notification requirements, or audit rights. VeriPulse has no mechanism to detect a security incident originating from a supplier before it affects the platform or client data.
Risk Implication	VeriPulse's API integrations with hospital systems create a supply chain risk surface both ways. A compromise of VeriPulse's platform could propagate to hospital systems, and a compromise of a hospital integration could affect VeriPulse's data integrity.

Requirement (e): Network & IS Security, Development & Maintenance	🟡 Partially Compliant
Current State	VeriPulse's infrastructure is hosted on Microsoft Azure, which provides a range of baseline security controls including network segmentation capabilities, DDoS protection, and platform-level vulnerability management. Some security tooling is available by default. However, there is no documented patch management policy and no defined vulnerability disclosure or tracking process
Required State	Article 21(2)(e) requires policies and procedures for the secure acquisition, development, and maintenance of network and information systems. This includes vulnerability handling, patch management, secure coding practices, and software security testing before deployment.
Gap	Azure's native controls provide a partial technical baseline, but VeriPulse has not documented how those controls are configured or maintained. No patch management policy exists. There is no defined process for tracking known vulnerabilities in platform dependencies.
Risk Implication	Unpatched vulnerabilities in platform dependencies represent a known and exploitable attack surface. The absence of pre-deployment security testing means that code changes could introduce vulnerabilities directly into a platform processing health-adjacent data. Reliance on cloud-provider defaults without documented governance does not ensure compliance.

Requirement (f): Effectiveness Assessment & Cybersecurity Testing	🔴 Non-Compliant
Current State	No formal process exists for evaluating the effectiveness of VeriPulse's security controls. No internal or external security audits have been conducted. No **Key Performance Indicators (KPIs)** or metrics related to security posture are tracked. No penetration testing or security review has been performed on the VeriPulse platform.
Required State	Article 21(2)(f) requires organisations to have processes for assessing the effectiveness of their cybersecurity risk-management measures. This includes periodic reviews, audits, and testing activities proportionate to the organisation's risk profile.
Gap	VeriPulse has no mechanism to determine whether its existing controls are functioning as intended. No audit history exists. Security effectiveness is entirely unmeasured. The IT Manager has no defined process for reviewing or reporting on the security posture of the organisation.
Risk Implication	Controls that are not tested cannot be relied upon. Without effectiveness assessment, VeriPulse cannot demonstrate to a regulator that its measures are proportionate and functioning. This gap also means that control degradation (e.g. lapsed configurations, expired certificates, unreviewed access) would go undetected.

Requirement (g): Cyber Hygiene & Security Training	🟡 Partially Compliant
Current State	No formal security awareness training programme exists. Staff have not received documented security awareness training. The IT Manager may communicate security guidance informally, but there is no structured programme, no training records, and no minimum training requirement for staff with access to production systems or sensitive data.
Required State	Article 21(2)(g) requires organisations to maintain basic cyber hygiene practices and to deliver security awareness training to all staff. Training must be commensurate with staff roles and access levels, and must cover topics including phishing awareness, password security, and incident reporting.
Gap	No training programme exists. No training records are maintained. Staff with access to sensitive patient-reported data and production systems have received no documented security awareness training. There is no onboarding security briefing process for new hires.
Risk Implication	Untrained staff represent a primary attack vector, particularly for phishing and social engineering attacks. A single compromised credential on a developer's account would provide access to Azure tenant administration or production data. The absence of training records also means VeriPulse cannot demonstrate a culture of security to regulators or clients during a post-incident review.

Requirement (h): Cryptography & Encryption	🟡 Partially Compliant
Current State	Microsoft Azure encrypts data at rest and in transit by default across its managed services. VeriPulse's platform therefore benefits from baseline encryption without explicit configuration. However, no cryptography policy exists. There is no documented governance of encryption standards, key management procedures, certificate lifecycle management, or rules governing encryption of data exported from the platform.
Required State	Article 21(2)(h) requires organisations to have documented policies on the use of cryptography and encryption, including key management. Encryption must be applied proportionately to data sensitivity, and the organisation must govern how cryptographic keys are managed, rotated, and retired.
Gap	Azure's default encryption provides a partial technical control, but VeriPulse has not documented it as a deliberate policy decision. No key management procedure exists. Certificate expiry monitoring is not in place. There is no policy governing encryption of data in transit between VeriPulse and its hospital clients via APIs.
Risk Implication	Undocumented reliance on cloud-provider defaults does not constitute a cryptography policy under Article 21. An expired TLS certificate on an API endpoint, or an unrotated encryption key, would represent a real exposure that VeriPulse currently has no process to detect or prevent. Unencrypted data transfers over FHIR API connections could also expose patient-related data during transmission.

Requirement (i): HR Security, Access Control & Asset Management	🟡 Partially Compliant
Current State	**Azure Active Directory (AAD)** is in use as the identity platform, providing a structural basis for access control. However, no formal access control policy exists. There is no documented **Joiners/Movers/Leavers (JML)** process. Privileged access to production systems is not formally governed. No complete asset inventory is maintained. There is no documented process for revoking access upon employee departure.
Required State	Article 21(2)(i) requires organisations to have documented policies for human resources security, access control, and asset management. This includes a defined process for granting, reviewing, and revoking access; role-based access control principles; and a maintained inventory of all network and information system assets.
Gap	**Azure Active Directory (AAD)** provides the technical capability for access control, but VeriPulse has not implemented a formal access governance process on top of it. No asset register exists. Access rights have not been formally reviewed. There is no defined process for revoking access when staff leave, creating a risk of persistent access by former employees. Privileged Azure tenant roles are not documented or periodically reviewed.
Risk Implication	Unmanaged access rights are a primary cause of insider threat and post-departure data exposure. Without a **JML** process, a departing developer retains Azure tenant access until manually revoked. Without an asset inventory, VeriPulse cannot assess the full scope of a security incident, as it does not have a complete picture of what systems and data exist.

Requirement (j): MFA & Secure Communications	🟡 Partially Compliant
Current State	Azure Active Directory supports **Multi-Factor Authentication (MFA)** and Conditional Access policies. However, **MFA** has not been enforced organisation-wide. Enforcement is inconsistent: some administrative accounts have **MFA** enabled, while developer accounts and external collaborator accounts do not. No policy mandating **MFA** for specific roles or access levels exists. Internal communications occur over Slack, which supports **MFA** but enforcement has not been verified.
Required State	Article 21(2)(j) requires organisations to use **Multi-Factor Authentication (MFA)** or continuous authentication solutions where appropriate, and to use secured voice, video, and text communications and secured emergency communication systems where necessary.
Gap	MFA is available but not enforced as a mandatory control. No policy defines which accounts, roles, or access scenarios require **Multi-Factor Authentication (MFA)**. Developer accounts with production access are not covered. There is no verification that communication platforms used for security-sensitive discussions (Slack, email) enforce MFA for all participants.
Risk Implication	A single compromised password on an unprotected developer account is sufficient to gain access to Azure production resources, source code, and patient-related data. **Multi-Factor Authentication (MFA)** enforcement is one of the most effective single controls against credential-based attacks. Its partial implementation creates an uneven perimeter where the weakest unprotected account defines the effective security boundary.

5. Risk Register

5.1 Scoring Framework

The following assessment scales are employed to evaluate the specific gaps identified in the previous section and to facilitate the formal construction of the risk register:

Likelihood scale:

- 1 — Unlikely: No known threat vector, extremely unlikely to be exploited.
- 2 — Possible: Known vectors exist but exploitation requires significant effort.
- 3 — Likely: Exploitation is straightforward given the current control posture.
- 4 — Almost certain: Active exploitation is highly probable in the absence of any control.

Impact scale:

- 1 — Negligible: Minimal operational or reputational effect; no regulatory consequence.
- 2 — Minor: Limited disruption; recoverable without significant efforts.
- 3 — Significant: Material service disruption, client notification required.
- 4 — Severe: Prolonged outage, may cause large scale incident.

Impact \ Likelihood	L = 1	L = 2	L = 3	L = 4
I = 4	4	8	12	16
I = 3	3	6	9	12
I = 2	2	4	6	8
I = 1	1	2	3	4

Score = Impact x Likelihood

Score	Level	Rating	Meaning
12 – 16	🔴 Critical	Immediate action required	Unacceptable risk. Must be mitigated before Cbw enforcement. No tolerance.
8 – 11	🟠 High	Prioritise within 30–60 days	Significant risk requiring planned remediation. Acceptable only possible with mitigation plan.
4 – 7	🟡 Medium	Address within 60–90 days	Manageable risk. Should be addressed within the remediation roadmap horizon.
1 – 3	🟢 Low	Address within 90-180 days	Low risk. Should be addressed whenever is convenient and or the resources are available..

5.2 Risk Summary

Total Risks	🔴 Critical	🟠 High	🟡 Medium
12	6	5	1

The risk profile reflects an organisation with a foundational governance deficit, lacking the underlying structure of policy and documentation in addition to the lack of technical controls.

- The six Critical risks are not isolated technical vulnerabilities, they represent structural absences: no policy, no incident plan, no disaster recovery, no MFA enforcement, and no reporting capability. Each of these would cause independent regulatory violations under the Cyberbeveiligingswet, regardless of whether a security incident occurs.

- The four High risks represent controls that are technically available but not governed or enforced. These are the fastest to remediate once the governance framework from Critical risks is in place.

- The single Medium risk (R-12, cryptography) is partially mitigated by Azure defaults. It requires formalisation rather than implementation from scratch, and can realistically be addressed within the 90-day roadmap horizon.

5.3 Risk Register

ID	Risk Title	Description	Likelihood	Impact	Score	Owner	Treatment
R-01	**Absence of Information Security Policy**	No IS Policy exists. Without a documented policy, VeriPulse cannot demonstrate a governance framework to regulators, clients, or auditors. All other controls lack a policy basis.	**4**	**4**	**16** 🔴 Critical	Board / CTO	Mitigate
R-02	**No Formal Risk Assessment Conducted**	Risks to network and information systems have never been formally assessed. Control selection is arbitrary. The possibility of zero-day exploits is high.	**4**	**3**	**12** 🔴 Critical	CTO / IT Manager	Mitigate
R-03	**No Incident Response Plan**	VeriPulse has no documented cybersecurity incident response procedure. In the event of a breach or disruption, response would be uncoordinated and the NIS2 24-hour reporting deadline would almost certainly be missed.	**3**	**4**	**12** 🔴 Critical	CTO	Mitigate
R-04	**Failure to Meet NIS2 Incident Reporting Obligations**	Missing the early warning deadline is an independent regulatory violation regardless of how the underlying incident is handled.	**3**	**4**	**12** 🔴 Critical	CTO / Legal	Mitigate
R-05	**No Tested Disaster Recovery Capability**	No DRP exists and no recovery test has been conducted. Azure backups are unconfigured beyond defaults. In a destructive attack or critical failure, recovery time and data loss cannot be certain.	**3**	**4**	**12** 🔴 Critical	IT Manager	Mitigate
R-06	**Unassessed Third-Party Supply Chain Risk**	No supplier security assessments have been conducted. Vendor contracts contain no security obligations or breach notification clauses.	**3**	**3**	**9** 🟠 High	CTO / IT Manager	Mitigate

ID	Risk Title	Description	Likelihood	Impact	Score	Owner	Treatment
R-07	**Absence of Patch Management Process**	No policy or process governs patching of platform dependencies, OS-level components, or third-party libraries. Known vulnerabilities in production dependencies may go undetected and unresolved.	**3**	**3**	**9** 🟠 High	IT Manager	Mitigate
R-08	**No Security Effectiveness Measurement**	No audits, KPIs, or testing activities exist to verify that controls are functioning. Control degradation would go undetected.	**3**	**3**	**9** 🟠 High	CTO	Mitigate
R-09	**Untrained Staff Vulnerable to Social Engineering**	No security awareness training has been delivered. Phishing and social engineering represent the primary initial access vector for the vast majority of breaches.	**3**	**3**	**9** 🟠 High	CTO / HR	Mitigate
R-10	**No JML Access Process**	No formal process exists for granting or revoking system access. Departing employees may retain active Azure AD credentials and production system access indefinitely if manual revocation is overlooked.	**3**	**3**	**9** 🟠 High	IT Manager	Mitigate
R-11	**MFA Not Enforced on Developer and Production Accounts**	MFA is available in Azure AD but not mandated. Developer accounts with production access are unprotected.	**3**	**4**	**12** 🔴 Critical	IT Manager	Mitigate
R-12	**Cryptography and Key Management**	Encryption is partially provided by Azure defaults but is ungoverned. No key rotation policy, no certificate lifecycle management, and no policy covering API transport encryption exist.	**2**	**3**	**6** 🟡 Medium	IT Manager	Mitigate

6. Remediation Roadmap

This section translates the risk register in Section 5 into a sequenced, actionable remediation plan. Actions are organised across three phases based on risk priority. Each action includes a named owner, estimated effort, and a specific, verifiable success criterion.

All Phase 1 actions must be completed before the Cyberbeveiligingswet enters into force. Phases 2 and 3 should proceed concurrently with Phase 1 where resource permits, but the sequencing reflects minimum acceptable priority.

6.1 Phase Summary

Phase	Timeline	Risk Level	Actions	Objective
Phase 1	Days 1–30	🔴 **Critical**	5	Establish governance baseline. Close all regulatory zero-tolerance gaps.
Phase 2	Days 31–60	🟠 **High**	5	Formalise and enforce existing technical capabilities. Reduce attack surface.
Phase 3	Days 61–90	🟡 **Medium**	1	Document and govern partial controls. Achieve full Article 21 coverage.

6.2 Remediation Actions

Success criteria are the minimum evidence required to close the action.

Risk	Priority	Action	Owner	Time	Success Criterion
PHASE 1 — Days 1–30 | Critical Risks | Must complete before Cbw enforcement					
R-01	🔴 **Critical**	Draft and obtain board approval for an Information Security Policy covering scope, risk appetite, roles and responsibilities, acceptable use, and review cycle.	CTO + Board	2 weeks	Signed IS Policy document.
R-02	🔴 **Critical**	Conduct a formal risk assessment of VeriPulse's network and information systems using this register as the baseline. Document methodology, assumptions, and residual risks.	CTO / IT Manager	2 weeks	Completed risk assessment document linked to IS Policy.
R-03	🔴 **Critical**	Author and distribute an Incident Response Plan (IRP), including designated roles.	CTO	1 week	IRP document signed off with all relevant staff briefed.
R-05	🔴 **Critical**	Review and document Azure backup configurations. Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPOs) for VeriPulse's SaaS platform.	IT Manager	2 weeks	Backup config documented. RTO/RPO defined
R-11	🔴 **Critical**	Enforce MFA via Azure AD Conditional Access policy for all relevant accounts. No exceptions.	IT Manager	3 days	MFA enforcement confirmed via Azure AD audit log
PHASE 2 — Days 31–60 | High Risks | Complete with documented mitigation plans					
R-06	🟠 **High**	Conduct a security review of all critical third-party suppliers (Azure, AWS, Atlassian, Slack). Introduce security clauses and breach notification obligations into new and renewed vendor contracts.	CTO / Legal	3 weeks	Supplier security assessment log created. At least one vendor contract updated with security clauses.

Risk	Priority	Action	Owner	Time	Success Criterion
R-07	🟠 **High**	Define and document a patch management policy. Implement automated dependency vulnerability scanning on all production code repositories.	IT Manager	2 weeks	Patch management policy signed off Vulnerability scanner active on all repositories
R-08	🟠 **High**	Define a set of security Key Performance Indicators (KPI's) to be reviewed monthly by the CTO within a set schedule.	CTO	1 week	Key Performance Indicator dashboard first monthly review scheduled and completed.
R-09	🟠 **High**	Deliver a mandatory security awareness training session to all staff covering phishing, password hygiene and incident reporting. Maintain attendance records.	CTO / HR	2 weeks	Training delivered.
R-10	🟠 **High**	Document and implement a Joiners / Movers / Leavers (JML) process in Azure AD. Conduct an immediate access review: revoke all unnecessary or legacy accounts. Document results.	IT Manager	1 week	JML process document published; access review completed and results documented; zero unaccounted for accounts confirmed.
PHASE 3 — Days 61–90 | Medium Risks | Formalise existing partial controls					
R-12	🟡 **Medium**	Document VeriPulse's cryptography policy, covering: Azure encryption standards in use, TLS requirements for API connections, key rotation schedule, and certificate expiry monitoring. Implement certificate expiry alerting.	IT Manager	1 month	Cryptography policy document approved; certificate monitoring alert configured; key rotation schedule defined.

6.3 Post-Roadmap: Maintaining Compliance

Completing this roadmap brings VeriPulse to a baseline NIS2-compliant posture. Maintaining this posture requires the following activities to be embedded into normal operations:

- **Monthly:** CTO security Key Performance Indicators review.
- **Quarterly:** IS Policy and risk register review; access rights review; supplier security.
- **Annually:** Full internal gap analysis against NIS2; security awareness training .
- **Trigger-based:** Repeat risk assessment following any significant change to systems.

VeriPulse should also complete voluntary registration with National Cyber Security Centre (NCSC) as an early action in Phase 1, independent of the Cbw's formal entry into force. This demonstrates proactive intent, and establishes the NCSC relationship before it is needed in an emergency.

7. Incident Reporting Procedure

This section constitutes VeriPulse B.V.'s operational incident reporting procedure, drafted in accordance with Article 23 of the NIS2 Directive and the forthcoming Cyberbeveiligingswet. It is intended for immediate distribution to relevant staff and for adoption as a standing operating procedure upon board approval.

Disclaimer: *Pending board approval. Until formally adopted, this procedure should be treated as operational guidance.*

7.1 Purpose and Scope

This procedure defines how VeriPulse B.V. detects, classifies, escalates, and reports cybersecurity incidents affecting its network and information systems. It applies to all VeriPulse staff, contractors, and third parties with access to VeriPulse systems.

A 'significant incident' for the purposes of NIS2 Article 23 reporting is one that causes or is capable of causing any of the following:

- **Serious operational disruption to VeriPulse's services**
- **Financial losses to VeriPulse**
- **Significant material or immaterial damage to other organisations**

7.2 Incident Classification

Severity	Label	Example Triggers	Reporting Obligation
P1	**Critical**	Platform fully unavailable, confirmed data breach, ransomware, API compromise.	NCSC-NL early warning within 24h. 72h notification. 30-day final report. Notify affected third parties immediately.
P2	**High**	Partial service degradation; suspected breach under investigation; significant data integrity issue	Assess within 2h. If confirmed significant: NCSC-NL early warning within 24h of confirmation.
P3	**Medium**	Failed login spike; isolated malware on endpoint; data quality anomaly with no confirmed breach	Log and investigate. Escalate to P2/P1 if evidence of compromise. No mandatory external reporting unless escalated.
P4	**Low**	Security policy violation; minor configuration drift; non-critical vulnerability identified	Log in the incident register. Assign remediation owner. Review at next monthly security review.

7.3 Escalation Contacts

The following contacts must be notified based on escalation triggers defined in 7.2. All contact details must be kept current. The IT Manager must review this table quarterly.

Role	Name / Contact	Responsibility	When to Escalate
IT Manager	[Name] — [email] — [phone]	First responder. Initial triage, containment actions, internal escalation.	Immediately upon detection of any P1 or P2 event.
CTO	[Name] — [email] — [phone]	Incident commander for P1/P2. Authorises external communications and regulatory notifications.	Within 1 hour of IT Manager escalation for P1/P2.
CEO / Board	[Name] — [email] — [phone]	Executive oversight. Approves client and regulatory notification content.	For all P1 incidents and any P2 involving potential data breach.
External DPO	[Name] — [email] — [phone]	Advises on GDPR notification obligations. Coordinates with AP (Autoriteit Persoonsgegevens) if personal data is affected.	For any incident where patient-related data may have been accessed or exfiltrated.
Legal Counsel	[Name / Firm] — [phone]	Advises on regulatory and contractual obligations. Review all external notifications before sending.	For all P1 incidents before any external communication is issued.

NCSC-NL Incident Portal: https://www.ncsc.nl/contact/kwetsbaarheid-melden | Emergency line: +31 70 888 7555

7.4 Step-by-Step Response Procedure

Step 1: Detect & Log (T = 0)

1. Any staff member who identifies a potential security incident must immediately report it to the IT Manager by phone (Email alone insufficient).
2. The IT Manager logs the incident in the VeriPulse Incident Register, recording: date/time of detection, reporter name, initial description of the event, and affected systems.
3. The IT Manager performs an initial classification of the incident as P1, P2, P3, or P4 using the classification table.

Step 2: Contain (T + 0 to 2h)

4. For P1 and P2: the IT Manager initiates immediate containment actions proportionate to the incident type. This may include isolating affected systems, revoking compromised credentials, or disabling affected API connections.
5. Containment actions must not destroy forensic evidence. Where possible, take a snapshot or preserve logs before isolating systems.
6. The IT Manager escalates to the CTO within 1 hour of initial classification as P1 or P2.

Step 3: Assess Significance (T + 1 to 4h)

7. The CTO, in consultation with the IT Manager and where applicable the external DPO, assesses whether the incident meets the threshold of a 'significant incident' under NIS2 Article 23.
8. If the incident is assessed as significant, or if significance cannot be ruled out, proceed immediately to Step 4. Do not wait for a full investigation before filing the early warning.
9. Document the significance assessment rationale in the incident register regardless of the outcome.

Step 4: Early Warning to NCSC-NL (Before T + 24h)

10. The CTO submits an early warning via the NCSC-NL incident portal within 24 hours of first detecting or suspecting a significant incident.
11. The early warning must include: incident type and nature, initial scope assessment, any suspected cross-border impact, and whether the cause is known. It does not need to be complete or conclusive.
12. Legal counsel must be notified before submission. If legal counsel cannot be reached within 2 hours, proceed with submission, the 24-hour deadline is absolute.
13. Retain a copy of the submission and NCSC-NL timestamp confirmation.

Step 5: Investigate & Notify Clients (T + 24 to 72h)

14. Continue investigation to determine root cause, full scope, and impact on client data and services.
15. If patient-related data has been accessed or exfiltrated, the external DPO must notify the Autoriteit Persoonsgegevens (AP) within 72 hours under GDPR Article 33.

Step 6: 72-Hour Notification (Before T + 72h)

16. The CTO submits the updated incident notification to NCSC-NL via the portal, retaining a copy and timestamp confirmation.

Step 7: Remediate & Document (T + 72h to 30 days)

17. The IT Manager leads remediation of the root cause, with the CTO overseeing progress.
18. All remediation actions are logged in the incident register with dates and outcomes.
19. The incident register entry is updated continuously throughout this phase.

Step 8: Final Report (Before T + 30 days)

20. The CTO authors a final incident report covering: confirmed root cause, full impact assessment, complete timeline, remediation actions taken, lessons learned, and any changes made to controls or procedures.
21. The final report is submitted to NCSC-NL, presented to the board, and retained in VeriPulse's records for a minimum of five years.
22. If the incident resulted in changes to this procedure, a revised version must be approved by the board within 60 days.

7.5 NIS2 Reporting Timeline Reference

Deadline	Obligation	Required Content	Recipient
T + 24h	**Early Warning**	Notification that a significant incident has occurred or is suspected. Incident type, initial assessment of scope, any known cross-border impact. Does not need to be comprehensive.	NCSC-NL via the NCSC incident portal. CTO is the notification owner.
T + 72h	**Incident Notification**	Updated assessment including: initial cause assessment, affected systems and services, estimated number of users/clients affected, containment measures taken, ongoing investigation status.	NCSC-NL (update to initial report). Affected hospital and pharma clients where service disruption is confirmed. External DPO if personal data is involved.
T + 30 days	**Final Report**	Full incident report including: root cause analysis, full impact assessment, remediation actions taken, lessons learned, and any changes made to controls or procedures as a result.	NCSC-NL (final report). Board. Affected clients if applicable. Retained for internal audit record.

8. Conclusion

The gap analysis confirms that VeriPulse B.V. currently operates with a foundational deficit in cybersecurity governance and structural controls. As an Important Entity under NIS2, the absence of a documented Information Security Policy and Incident Response Plan creates a significantly weak security posture that is open to being exploited by malicious actors and foreign nationals. Non-compliance with the forthcoming Cyberbeveiligingswet (Cbw) poses severe risks, including administrative fines of up to €7 million and potential personal liability for board members.

The three-phase remediation roadmap provides a structured path toward achieving full compliance. Immediate action is required in Phase 1 to establish the necessary governance baseline and mitigate critical risks before active enforcement begins. By systematically addressing these gaps, VeriPulse will not only satisfy its regulatory obligations under NIS2 but also significantly enhance the resilience of its SaaS platform and the protection of sensitive patient-related data.

— End of Document —