MIROSLAV TADEJ CONSULTING

Information Security Policy

Information Security Management System (ISMS)

Aligned with ISO/IEC 27001:2022 · GDPR & Data Protection Act 2018 · OWASP secure-development practice

Document control

Document title	Information Security Policy
Document owner	Miroslav Tadej, Principal Consultant (ISMS Owner)
Organisation	Miroslav Tadej Consulting
Version	1.0
Status	Approved
Classification	Public — issued for tender and client assurance
Effective date	13/06/2026
Next review date	12/06/2027
Approved by	Miroslav Tadej, Principal Consultant

Revision history

Version	Date	Summary of change	Author
1.0	[Insert]	Initial issue of the Information Security Policy.	M. Tadej

Contents

1. Purpose

This Information Security Policy establishes the principles, objectives, and responsibilities by which Miroslav Tadej Consulting ("the Consultancy") protects the confidentiality, integrity, and availability of information assets — its own and those entrusted to it by clients. It forms the top-level policy of the Consultancy's Information Security Management System (ISMS) and sets the direction for all subordinate policies, procedures, and controls.

The Consultancy designs, builds, secures, and maintains web applications for clients across the private and public sectors in Ireland. Because client systems frequently process personal data and support business-critical operations, robust information security is fundamental to the service the Consultancy provides and to the trust placed in it.

2. Scope

This policy applies to all information assets owned, processed, or managed by the Consultancy, in every format and location, throughout their lifecycle. It covers:

- all information created, received, stored, processed, or transmitted in the course of the Consultancy's business, including client data and source code;
- all information systems, applications, cloud services, development environments, devices, and networks used to deliver services;
- the Principal Consultant and any contractor, subcontractor, or third party who accesses the Consultancy's or a client's information assets under the Consultancy's direction; and
- all engagements, whether delivered on the Consultancy's infrastructure or within a client's environment.

Where the Consultancy acts as a data processor on behalf of a client (the data controller), this policy operates alongside the relevant data-processing agreement and the Consultancy's Data Protection Policy.

3. Policy statement and objectives

The Consultancy is committed to protecting the information assets within its care and to operating a security posture appropriate to the risks faced by a specialist cybersecurity and software-development practice. The Consultancy adopts a "Secure by Design" philosophy: security is built into systems and processes from the outset rather than added afterwards.

The objectives of this policy are to:

1. preserve the confidentiality of information, ensuring it is accessible only to those authorised to have access;
2. maintain the integrity of information, safeguarding its accuracy and completeness;
3. ensure the availability of information and services to authorised parties when required;
4. meet all applicable legal, regulatory, and contractual obligations, including the GDPR, the Data Protection Act 2018, and obligations arising under client contracts and public-sector tenders;
5. manage information-security risk through a structured, documented, and regularly reviewed process; and
6. continually improve the ISMS in line with evolving threats, technologies, and the Consultancy's obligations.

This policy is aligned with the control framework of ISO/IEC 27001:2022, whose 93 Annex A controls are grouped into four themes — organisational, people, physical, and technological. The Consultancy applies the controls relevant to its risk profile; control applicability is recorded and reviewed as the practice grows.

4. Roles and responsibilities

As a sole-practitioner consultancy, the Principal Consultant holds overall and ultimate accountability for information security. The following responsibilities are defined and, where the practice engages contractors, are allocated accordingly:

Role	Responsibilities
Principal Consultant (ISMS Owner)	Owns this policy and the ISMS; approves policies; sets risk appetite; ensures legal and contractual compliance; conducts risk assessments and reviews; acts as the primary contact for security and data-protection matters.
Data protection lead	Held by the Principal Consultant: oversees GDPR compliance, data-subject requests, and breach handling (see Data Protection Policy).
Contractors / subcontractors	Comply with this policy and all subordinate policies; complete any required confidentiality agreements; report security events without delay.
Clients	Where the Consultancy processes data on their behalf, define the scope and instructions for processing through a data-processing agreement.

5. Information security risk management

The Consultancy manages information-security risk through a documented, repeatable process. Risks to the confidentiality, integrity, and availability of information assets are identified, analysed, evaluated against the Consultancy's risk appetite, and treated through the selection of appropriate controls.

5.1 Risk approach

- **Risk register:** Risks are recorded in a risk register, each with an owner, an assessed likelihood and impact, and a treatment decision.
- **Treatment:** Risk treatment follows the standard hierarchy — modify (apply controls), retain (accept), avoid, or share (e.g. via insurance or supplier contract).
- **Review:** The risk register is reviewed at least annually and whenever a significant change occurs — a new service, a new client environment, a material change in the threat landscape, or a security incident.

Controls are selected primarily from ISO/IEC 27001:2022 Annex A and supplemented by OWASP guidance for application security. Residual risk is reviewed and explicitly accepted by the Principal Consultant.

6. Information classification and handling

Information is classified so that protection is proportionate to sensitivity. The Consultancy uses four levels:

Classification	Description	Handling
Public	Information approved for release, e.g. marketing material and these governance documents.	No restriction on distribution.
Internal	Business information not intended for public release, e.g. proposals and internal notes.	Shared on a need-to-know basis.
Confidential	Client data, source code, credentials, and personal data.	Encrypted at rest and in transit; access strictly controlled.
Restricted	Highly sensitive material, e.g. security-test findings and secrets.	Strongest controls; minimal access; encrypted and segregated.

Personal data is treated as Confidential or Restricted and handled in accordance with the Data Protection Policy and GDPR. Information is retained only as long as necessary and securely destroyed when no longer required.

7. Access control and authentication

Access to information and systems is granted on the principles of least privilege and need-to-know, and is removed promptly when no longer required.

- **Identity:** Unique credentials are used for each system; shared accounts are avoided. Access rights are reviewed periodically.
- **MFA:** Multi-factor authentication (MFA) is enabled on all accounts that support it, including code repositories, cloud consoles, email, and administrative interfaces.
- **Passwords:** Strong, unique passwords are enforced and managed through a reputable password manager; credentials are never stored in source code or in plaintext.
- **Application auth:** In applications built by the Consultancy, authentication uses industry-standard mechanisms — for example JSON Web Tokens carried in httpOnly cookies, with passwords hashed using bcrypt — and authorisation is enforced through role-based access control at both the route and data layers.

8. Cryptography

Encryption protects information in transit and at rest. All web services are delivered over TLS (HTTPS), with plain-HTTP redirected to HTTPS. Data at rest on managed databases and storage is encrypted using provider-managed encryption. Secrets and cryptographic keys are stored in dedicated secret stores or environment configuration, never committed to source control. Password storage uses strong, salted one-way hashing.

9. Operations security

9.1 Malware protection

Endpoints used to deliver services run reputable, up-to-date anti-malware protection, and software is kept current with security patches.

9.2 Patch and vulnerability management

Operating systems, applications, and software dependencies are kept up to date. Dependencies are monitored for known vulnerabilities using automated scanning (for example dependency-alerting tools), and security-relevant updates are applied promptly and prioritised by severity.

9.3 Logging and monitoring

Security-relevant events — authentication, administrative actions, and errors — are logged. Production systems use centralised, structured logging and error monitoring, and logs are reviewed to detect anomalous or unauthorised activity. Logs are protected against tampering and retained for an appropriate period.

9.4 Backup

Critical information and client systems are backed up. Backups are encrypted, stored securely, and tested by restore so that recovery objectives can be met. Backup and recovery arrangements are described further in the Business Continuity & Disaster Recovery Plan.

10. Network and physical security

Production environments restrict inbound access to only the ports and origins required; databases are not exposed publicly; and cross-origin access is limited to known client origins. Security headers and a content-security policy are applied to web applications. Working devices are protected by full-disk encryption, automatic screen locking, and a clear-desk and clear-screen practice. Devices and removable media are physically secured, and equipment is securely wiped before disposal or reuse.

11. Secure development

Because software development is central to the Consultancy's service, secure development is a core control area. Applications are built following "Secure by Design" principles and the OWASP Top 10,

including parameterised database queries to prevent injection, validated and sanitised input, secure session and token handling, least-privilege authorisation, and protection of payment flows through PCI-compliant providers so that card data never resides on Consultancy or client servers. Detailed requirements are set out in the Secure Development Policy.

12. Supplier and third-party security

The Consultancy relies on third-party providers — cloud hosting, source-code hosting, payment processing, email, and monitoring. Suppliers are selected with regard to their security posture and compliance credentials. Where a supplier processes personal data on behalf of the Consultancy or its clients, an appropriate data-processing agreement is put in place, consistent with Article 28 of the GDPR. Supplier access to Consultancy or client information is limited to what is necessary.

13. Information security incident management

The Consultancy maintains the capability to detect, report, assess, and respond to information-security events and incidents.

7. Suspected events are recorded and assessed without delay to determine whether an incident has occurred and its severity.
8. Incidents are contained, eradicated, and recovered from, with actions documented throughout.
9. Where an incident involves personal data, the breach-handling process in the Data Protection Policy is followed, including notification to the Data Protection Commission within 72 hours where the breach is likely to result in a risk to individuals, and to affected clients and data subjects where required.
10. Each significant incident is followed by a review to identify root cause and improvements, which are fed back into the risk register and controls.

14. Business continuity

The Consultancy maintains arrangements to continue delivering critical services and to recover information and systems following a disruption. These arrangements, including recovery objectives, backup strategy, and supplier-failure scenarios, are documented in the Business Continuity & Disaster Recovery Plan, which supports this policy.

15. Legal, regulatory, and contractual compliance

The Consultancy complies with all information-security and data-protection obligations applicable to its work in Ireland, including:

- the General Data Protection Regulation (EU 2016/679) and the Data Protection Act 2018, regulated by the Data Protection Commission;
- the ePrivacy Regulations governing electronic communications and the use of cookies;
- evolving national cybersecurity law, including measures transposing the EU NIS2 Directive through Ireland's forthcoming National Cyber Security Bill, which the Consultancy monitors so that its practice and that of its clients remain aligned; and
- security and assurance requirements arising from client contracts and public-sector procurement.

Intellectual property rights and licensing obligations in software and dependencies are respected. The Consultancy keeps these governance documents current as the legal landscape changes.

16. Awareness and competence

The Principal Consultant maintains current professional competence in cybersecurity through formal qualification at NFQ Level 9 and ongoing professional development. Any contractor engaged by the Consultancy is made aware of, and required to comply with, this policy and its subordinate policies before being granted access to information assets.

17. Policy monitoring, review, and continual improvement

This policy is reviewed at least once every twelve months, and additionally following any significant change to the Consultancy's services, technology, risk profile, or the legal and regulatory environment, or in response to a significant security incident. Reviews assess the policy's continued suitability, adequacy, and effectiveness, and result in documented improvements to the ISMS. The Consultancy is committed to the continual improvement of its information-security posture.

18. Breach of this policy

Any breach of this policy is taken seriously. Breaches by contractors or third parties may result in withdrawal of access and termination of engagement, and, where appropriate, referral to the relevant authorities. Breaches involving personal data are handled under the Data Protection Policy.

19. Related documents

- Data Protection Policy
- GDPR Compliance Statement
- Secure Development Policy
- Business Continuity & Disaster Recovery Plan
- Quality Management Statement

20. Approval

This Information Security Policy is approved and issued by the Principal Consultant of Miroslav Tadej Consulting and takes effect from the effective date recorded in the document-control table above.

Name & role	Signature	Date
Miroslav Tadej Principal Consultant	Miroslav Tadej	13/06/2026