

Information Security Policy v1.0

How We Keep This Policy Relevant

To show our commitment to this policy, we believe in full transparency. This isn't just a document that sits on a shelf; it's a living promise that we actively maintain, review, and support.

Property	Details
Our Policy Champion (Owner)	Windy Chan
Our Leadership Commitment (Approved by)	
Our Current Version	1.0
Effective From	
Keeping it Relevant (Next Review)	25/11/2026
Who This is For (Classification)	This is an Internal document, built for our entire EEZE team
Our Data Lifecycle (Retention)	We manage this policy's lifecycle according to the Retention & Disposal Schedule
Our Reference ID	EEZE-ISP-001

Leadership Keynote

At EEZE, security is how we protect our players, our people, and our purpose. We earn this trust not just with our words, but through risk-driven controls, continuous monitoring, and ISO-aligned accountability.

In the iGaming industry, trust is everything. Our players trust us with their data, our partners trust us with their reputation, and our teams trust that the systems they use are safe and reliable. Security isn't limited to compliance; it's how we embed responsibility and innovation together. Every one of us plays a role in keeping EEZE resilient and respected.

– *Director of Legal & Compliance*

1. Our Security Promise

At EEZE, we believe **security is everyone's responsibility**, it empowers us to operate confidently, innovate without barriers, and protect what matters most: our people, our data, and our brand.

Our Information Security Management System (ISMS) is aligned with ISO/IEC 27001:2022, providing a structured framework to safeguard the confidentiality, integrity, and availability of information.

Through continuous improvement, we strengthen our resilience and uphold the trust placed in us by our partners and customers.

2. Why It Matters

Our reputation and success depend on trust, built through independently verified controls and transparent compliance practices.

In a landscape where cyber threats evolve daily, even a single lapse can have significant impact. A strong security culture protects not only EEZE as a company, but also each of us, our work, our ideas, and our shared future.

By taking ownership of information security in everything we do, we safeguard the freedom to grow, create, and lead in our industry.

3. What This Means for You

This policy applies to everyone at EEZE - all employees, contractors, and third-party partners - who creates, processes, stores, shares, or disposes of company information.

The scope covers all company information, regardless of format (digital or physical) or storage location (on-premises, cloud-hosted, or hybrid).

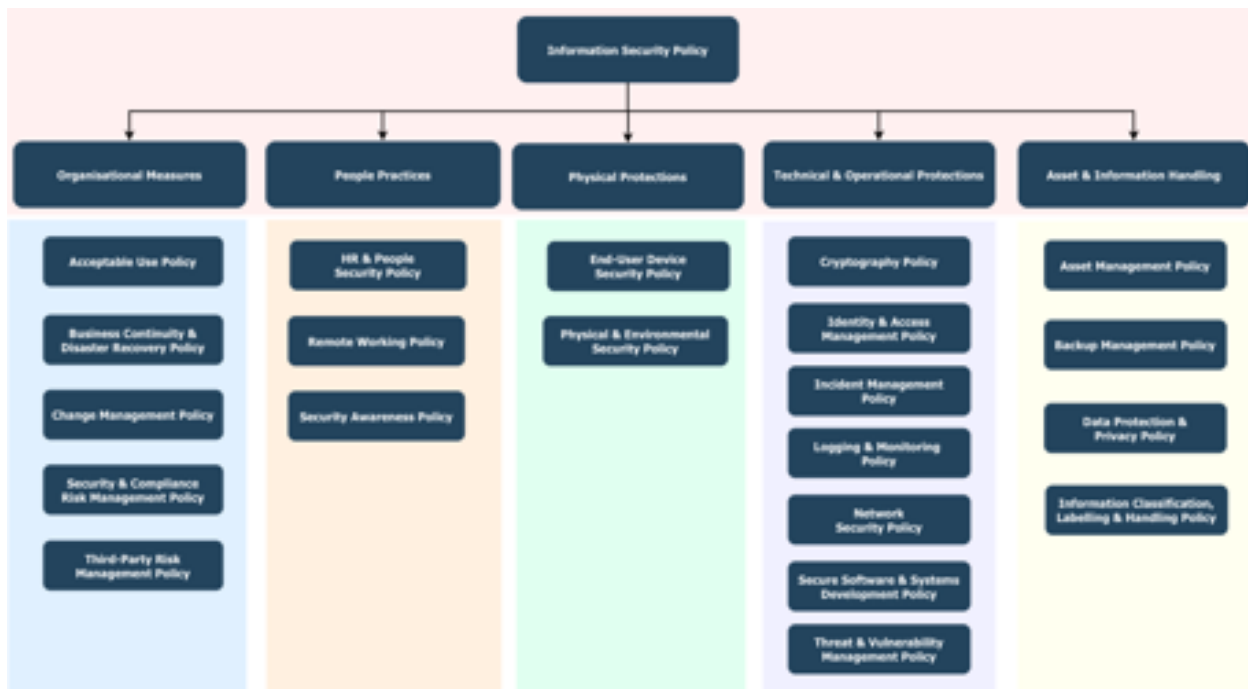
Whether you're in the office or working remotely, your actions are key to protecting our data throughout its entire lifecycle.

4. Our Approach to Security

We manage information security through a structured ISMS that blends technology, governance, and culture.

Our approach is built around five key themes:

1. **Organisational Measures** – governance, risk, and third-party management
2. **People Practices** – HR, awareness, and remote work
3. **Physical Protections** – facilities and device security
4. **Technical & Operational Protections** – system and network controls
5. **Asset & Information Handling** – data classification, privacy, and lifecycle management



5. Our Roles

We all have a part to play in keeping EEZE safe.

- **Leadership (Senior Executive Team):** The senior leaders are fully committed to our security. They are accountable for the ISMS, provide the resources to make it effective, and ensure our security goals align with our business strategy.
- **Governance Teams (Technical Compliance, ISMS Governance):** Think of the ISMS & Governance and Technical Compliance teams as your expert partners. They are responsible for designing and monitoring our security framework, helping us prepare for audits, and guiding us through security challenges.
- **Technical Teams (IT, DevOps, Engineering):** The technical teams are the expert implementers. They build, maintain, and secure the systems, networks, and technical controls that our security framework relies on.
- **You (Employees, Contractors, and Partners):** You are the front line of our security. Your responsibility is to understand and follow these security guidelines in your daily work. By reporting suspicious activity, handling data with care, and completing your training, you directly protect our company, our customers, and your colleagues.

Accountability: To maintain fairness and transparency, any policy breach or non-compliance is reviewed by ISMS Governance, with corrective actions coordinated in partnership with HR and Legal & Compliance, as appropriate.

6. How We Protect Our Business

6.1 Governance, Risk & Compliance

Why It Matters: We must anticipate risks, not react to them. By aligning our strategy with ISO/IEC 27001:2022, we ensure every control supports trust, regulatory compliance, and organizational resilience.

Key Takeaways:

- **ISMS as the Command Structure:** The Information Security Management System (ISMS) framework governs how we centrally manage, monitor, and continuously improve security across the organisation.
 - **Accountability Mandates:** Regular audits, comprehensive risk assessments, and executive management reviews are mandatory processes that keep us accountable and prove the effectiveness of our controls.
 - **Compliance as Credibility:** Compliance isn't a checkbox - it's how we earn the credibility to operate in every market and maintain the strategic trust of our players and partners.
-

6.2 People Security

Why It Matters: Our people are the heart of our defence. Awareness and action are key human factors that complement our technical and procedural defences. A strong security culture protects not only EEZE as a company but also each of us, our work, our ideas, and our shared future.

Key Takeaways:

- **Continuous Education:** Everyone completes security awareness training as part of onboarding, and continues to receive regular refreshers to stay current with emerging threats and best practices. Our complete training program, including role-specific requirements and compliance tracking, is detailed in our *Security Awareness Policy*.
 - **Active Vigilance:** Be alert to phishing, social engineering, and data mishandling. Your personal judgment is the final control against complex attacks.
 - **Mandatory Digital Hygiene:** You must lock screens, protect passwords, and handle company devices responsibly. This enforces fundamental security standards across all personal endpoints
-

6.3 Asset & Data Protection

Why It Matters: Information is one of our most valuable assets. To protect it effectively, we must determine security requirements based on the data's sensitivity (classification) and the

importance of the assets that store it (criticality). Protecting both is critical for maintaining our reputation, ensuring compliance, and upholding our players' trust.

Key Takeaways:

- **First, Classify the Data:** All data is classified as Public, Internal, Confidential, or Highly Confidential based on its sensitivity and the impact if it were leaked.
- **Second, Determine Asset Criticality:** The data's classification directly determines the required asset criticality. Assets are assigned one of four criticality ratings (Supporting, Significant, Critical, or Highly Critical) as defined in the *Asset Management Policy*. By policy mandate, any asset (system, server, database) that stores or processes Highly Confidential data must be categorised as Highly Critical. Similarly, any asset storing or processing Confidential data must be categorised as Critical. This ensures the system receives the strongest protection controls necessary.

For example: A production database holding player data (Highly Confidential) is a Highly Critical Asset. A test server holding only anonymised, non-personal data (Internal) is a Supporting Asset.

- **Mandatory Handling:** You must store, share, and dispose of all data securely, strictly following the *Information Classification, Labelling, and Handling Policy*.
 - **Regulatory Alignment:** All personal data is protected in line with our *Data Protection & Privacy Policy*, ensuring legal and ethical stewardship.
-

6.4 Technology & Operations

Why It Matters: Technology drives our success - securing it keeps us available, compliant, and trusted. By enforcing operational discipline, we ensure the integrity of our systems and our data backbone.

Key Takeaways:

- **Patching and Configuration:** Apply software patches promptly, as outdated systems create risk. We mandate the use of secure baselines and controlled configurations across all infrastructure.
- **Access Control:** Strictly enforce Least Privilege and Need-to-Know access principles to prevent unauthorised access and lateral movement.
- **Secure Development:** All new software must be built using Security-by-Design principles, utilising secure coding standards and non-bypassable security gates in the deployment pipeline.
- **Incident Response:** Report incidents immediately - early action limits damage and supports system recoverability.
- **Network Integrity:** Maintain network segmentation (logical separation) between the corporate network and the production network, and others (guest network) and ensure all

sensitive traffic is encrypted in alignment with the *Cryptography Policy* to protect the digital backbone.

6.5 Third-Party Trust

Why It Matters: Every partner we work with extends our digital ecosystem. Their security is therefore our security. We must maintain constant vigilance because poor security practices by a single vendor can introduce significant, unmanaged risk into our network.

Key Takeaways:

- **Mandatory Lifecycle Governance:** We approve, monitor, and assess all third-party relationships to ensure they meet EEZE's security and compliance standards. This includes pre-engagement due diligence, robust contractual clauses, and periodic performance and security reviews, recognising that operational control ultimately resides with the vendor. These activities are governed by our *Third-Party Risk Management Policy*.
 - **Integrated Response and Reporting:** Any security issue, incident, or change that could affect EEZE's systems, data, or services must be immediately reported to the Third-Party Relationship Manager, who will coordinate the response in line with our *Third-Party Risk Management Policy*, *Change Management Policy*, and *Incident Management Policy*.
-

7. Your Role in Security

Everyone at EEZE has a part to play. You are:

- The **first line of defence** against threats.
- A **steward of trust** when handling assets and data.
- A **partner in improvement**, helping us make the ISMS stronger.

What You Can Do Today:

- Think before you click or share.
- Report anything suspicious - quickly and clearly.
- Ask when unsure - curiosity keeps us safe.

Remember: Security isn't just a rule, it's a shared responsibility. Your awareness and care keep us compliant and protect our reputation.

8. Our Approach to Accountability

Most security issues come from honest mistakes, not malicious intent. When something goes wrong, we start with curiosity: Why did this happen? Was the policy clear? Did you have the right training?

We focus on learning and fixing root causes. But if someone repeatedly ignores policies after coaching, or deliberately circumvents controls, we follow standard HR processes.

We're not trying to catch you out - we're trying to keep us all safe.

Speak Up: If something doesn't look right, talk to your manager, ISMS Governance, or Legal and Compliance. No penalty for good-faith concerns.

9. How We Measure Success

Security isn't only about prevention, it's about progress and effectiveness.

We measure success through clear, data-driven indicators that show how well our controls work in practice, not just that they exist. This includes the timely closure of audit findings, measurable reductions in security incidents linked to improved awareness, and responsive recovery times that meet or exceed service-level targets.

We also track training effectiveness, ensuring it leads to better security behaviour, not just high completion rates.

These indicators are reviewed and refined periodically to stay realistic, actionable, and aligned with EEZE's business objectives and risk environment.

9.1 Exception Management

In circumstances where compliance with this policy is not feasible, a formal exception may be requested. All exceptions must be documented, including the justification for the deviation, the risks created, and any proposed mitigating controls. Exceptions require approval from the Governance & Risk Officer and relevant management before implementation and are considered temporary, subject to periodic review.

Emergency deviations taken to protect the business must be documented within 48 hours and will be reviewed retrospectively. All approved exceptions are recorded in the Exception Register and managed in accordance with the *Security & Compliance Risk Management Policy* and the Exception Management Procedure.

10. Tools & Resources

You can find all related resources on *Confluence EEZE Management System Hub*.

11. Continuous Improvement

This policy evolves with our business, technology, and regulatory landscape. It is reviewed at least annually, and after any major organisational or technological change.

Your feedback is welcome (technicalcompliance@eeze.com) - security thrives when everyone contributes to making it stronger.

12. Key Takeaways

- **Shared Foundation:** Security is a shared responsibility - we all play a significant role in its success.
 - **Proactive Defence:** Awareness prevents incidents before they happen, turning every individual into a proactive defender.
 - **Core Discipline:** Strong processes and clear accountability protect our reputation, ensuring actions are traceable and governed.
 - **Strategic Integrity:** Compliance with this policy ensures regulatory and ethical integrity, safeguarding the trust of our players and partners.
 - **Cultural Mandate:** Security isn't just what we do - it's how we do everything, embedding resilience and responsibility into our business DNA.
-

13. Our Culture of Trust

Security isn't a barrier, it's the foundation for freedom, creativity, and progress. Every secure action we take strengthens EEZE, protects our players, and preserves our promise of fair, trusted gaming. Together, we don't just comply with security, we live it. This commitment embeds resilience and responsibility directly into our business DNA.

Our Record of Commitment

This policy is not a static document; it is a living commitment that evolves with our business, technology, and the threats we face. We believe in transparency and accountability, which is why we track every update and leadership approval. This log is our promise to you that we are continuously working on maintaining a reliable security posture, while retaining velocity.

ISMS Governance maintains this version history and ensures each update is reviewed and approved by Legal & Compliance.

Our Policy's Journey

Version	Date	Description of Change	Champion (Author)	Reviewer	Leadership Approval (Approver)
v1.0	25/11/2025	Policy creation	Windy Chan	Ryan Cachia	

Annex A: References

To aid in traceability and audits, this table maps the key control areas of ISO/IEC 27001:2022 to the core sections of this policy.

ISO 27001:2022 Control Area	Policy Section	Control Intent
A.5.1 (Policies for Information Security)	1 Our Security Promise	To ensure the organisation formally defines, approves, and commits to an Information Security Management System (ISMS), aligned with ISO/IEC 27001:2022, to safeguard the Confidentiality, Integrity, and Availability of all information assets
A.5.2 (Information Security Roles and Responsibilities)	5 Our Roles	To ensure top management accountability for the ISMS, and that security responsibilities for implementation, monitoring, and compliance are clearly defined and communicated to all technical teams and personnel across the organisation
A.5.4 (Management Responsibilities)	5 Our Roles	To ensure management actively supports information security through clear direction, commitment, and resource allocation
A.5.1 (Policies for Information Security), A.5.31 (Legal, Statutory, Regulatory and Contractual Requirements), A.5.36 (Compliance with Policies, Rules and Standards for Information Security)	6.1 Governance, Risk & Compliance	To establish a clear framework for management responsibility, risk, and compliance

A.6.1 (Screening), A.6.2 (Terms and Conditions of Employment), A.6.3 (Information Security Awareness, Education and Training), A.6.4 (Disciplinary Process), A.6.5 (Responsibilities After Termination or Change of Employment)	6.2 People Security	To manage human resource security and build a strong awareness culture
A.5.9 (Inventory of Information and Other Associated Assets), A.5.10 (Acceptable Use of Information and Other Associated Assets), A.5.12 (Classification of Information), A.5.13 (Labelling of Information), A.5.14 (Information Transfer)	6.3 Asset & Data Protection	To identify, classify, and protect information assets throughout their lifecycle

A.8.1 (User Endpoint Devices), A.8.2 (Privileged Access Rights), A.8.3 (Information Access Restriction) A.8.5 (Secure Authentication), A.8.9 (Configuration Management)	6.4 Technology & Operations	To protect systems and networks through secure configuration, access, and operations
A.5.19 (Information Security in Supplier Relationships), A.5.20 (Addressing Information Security Within Supplier Agreements), A.5.21 (Managing Information Security in the ICT Supply Chain), A.5.22 (Monitoring, Review and Change Management of Supplier Services)	6.5 Third-Party Trust	To manage the risks associated with third-party suppliers and partners

Note on Management Clauses: The core ISMS management requirements for Performance Evaluation (Clause 9) and Improvement (Clause 10) are addressed in the body of this policy, primarily in Section 8 (How We Measure Success) and Section 10 (Continuous Improvement).