**IMG Play ApS**

# INFORMATION SECURITY STATEMENT

| | |
|---|---|
| **Document Title:** | Information Security Statement |
| **Version:** | 2.2 |
| **Classification:** | Public |
| **Last Revised:** | December 12, 2025 |
| **Next Review:** | November 2026 (Annual) |
| **Approved by:** | Karsten Vandrup Westh, Chief Executive Officer |
| **Compliance Framework:** | NIS2 Article 21, D-mark Sections 1-8, ISO 27001, GDPR |

## 1. Our Commitment to Security

At IMG Play, we take information security seriously. As a technology integrator serving enterprise clients across Scandinavia and internationally, we understand the critical importance of protecting your data and maintaining the highest security standards.

This statement outlines our approach to information security and demonstrates our commitment to safeguarding the systems and data entrusted to us.

*Our commitment to quality, compliance, and security is not just a policy - it is our identity.*

## 2. What We Do

IMG Play is a technology integrator specializing in:

- Enterprise media workflows and platform integration
- Secure data transfer solutions and file acceleration
- Technical consulting and implementation services
- Cloud-based infrastructure solutions and management
- Platform management and technical support

**Important:** We do not process your end-user content. All customer content remains securely within your chosen enterprise platforms, managed by SOC 2 and ISO 27001 certified providers. IMG Play acts solely as a technical integrator and consultant.

## 3. Industry Recognition & Trust

**Entertainment Industry Validation:** IMG Play has successfully passed rigorous security audits from major Hollywood studios including Disney, Sony, Warner Bros., Universal, Paramount, and Fox - demonstrating our ability to protect the most sensitive media assets and intellectual property at the highest level.

These audits validate our comprehensive security controls, incident response capabilities, and commitment to protecting critical assets in high-security environments.

# 4. Our Security Framework

## 4.1 Access Control & Authentication

**Multi-Factor Authentication (MFA)**

MFA is mandatory across all IMG Play-controlled systems including:

- Enterprise productivity and collaboration suite
- Cloud storage and file sharing platforms
- Version control and development platforms
- Secure credential management systems
- Cloud hosting and infrastructure platforms
- Team communication tools
- Financial and payroll systems (using Danish MitID national identity)
- All administrative and management interfaces

**Access Management**

Key controls:

- Least privilege principle enforced across all systems
- Role-based access control: Executive, Management, Senior Technical, Technical
- Quarterly comprehensive access reviews
- Rapid offboarding procedures (within 1 hour for voluntary departures)
- Immediate access revocation for involuntary terminations
- No shared account policy - individual accountability enforced
- Centralized credential management with encryption and MFA protection

## 4.2 Data Protection

**Encryption Standards**

| Layer | Standard |
|---|---|
| **Data at Rest** | AES-256 encryption for all stored data, full disk encryption on all devices |
| **Data in Transit** | TLS 1.3 / TLS 1.2 for all network communications, HTTPS mandatory |
| **Development & Deployment** | Encrypted connections for all code transfers and deployments |
| **Backups** | Platform-native encryption for all backup storage |

**Data Classification System**

We maintain a 4-tier classification system with specific handling requirements:

| Classification | Examples | Access Control |
|---|---|---|
| **Public** | Marketing materials, public website content | Unrestricted |
| **Internal** | General business documents, team communications | Employees only |
| **Confidential** | Customer contracts, technical documentation, supplier agreements | Need-to-know basis |
| **Restricted** | Financial data, authentication credentials, employee personal data | Explicit management approval |

## 4.3 Infrastructure Security

### Zero Trust Architecture

We implement Zero Trust principles across our infrastructure:

- No trusted network zones - Every access attempt is verified regardless of origin
- Continuous verification of all access attempts with real-time validation
- Microsegmentation and least privilege enforcement
- Real-time monitoring with adaptive security policies
- Device security requirements: All devices must be encrypted, patched, and monitored
- Identity-centric security with strong authentication at every layer

### Cloud Security

All infrastructure and platform providers are:

- SOC 2 Type II or ISO 27001 certified (verified annually)
- Regularly audited for compliance by independent third parties
- Subject to our comprehensive Supplier Security Policy
- Required to maintain documented backup and recovery procedures
- Contractually obligated to 24-hour incident disclosure
- Reviewed quarterly for Category A (critical) suppliers

## 4.4 Continuous Monitoring

### 24/7 Security Monitoring

Our security monitoring includes:

- Real-time application and infrastructure monitoring
- Automated security scanning on every code change
- Daily automated dependency vulnerability scanning
- Automated credential leak detection and prevention
- Immediate alert escalation for critical security issues
- Weekly vulnerability reviews by technical leadership
- Log retention: 90 days for security events, extended for investigations

### Security Testing Tools

We employ industry-standard security testing tools including:

- Automated dependency scanning with daily updates
- Static Application Security Testing (SAST) on all code
- Automated secret scanning to prevent credential leaks
- Runtime monitoring and error detection systems
- Continuous integration security checks in deployment pipelines

**Vulnerability Management SLAs**

We maintain strict remediation timelines based on severity:

| Severity | CVSS Score | Remediation SLA | Escalation |
|---|---|---|---|
| **Critical (P1)** | 9.0-10.0 | 48 hours | CEO immediate notification |
| **High (P2)** | 7.0-8.9 | 7 days | CEO if not patched in 7 days |
| **Medium (P3)** | 4.0-6.9 | 30 days | Technical leadership oversight |
| **Low (P4)** | 0.1-3.9 | 90 days | Monthly review cycle |

**Target:** 100% of critical vulnerabilities remediated within 48 hours.

### 4.5 Incident Response

Comprehensive incident response procedures with P1-P4 severity classification. Response times: P1 <1 hour, P2 <4 hours. CEO notification immediate for P1 incidents. NIS2 regulatory timelines: 24-hour early warning, 72-hour full notification, 1-month final report. GDPR: 72-hour breach notification. Post-incident review within 7 days. 7-step workflow: Detection → Assessment → Notification → Containment → Eradication → Recovery → Closure.

### 4.6 Business Continuity & Disaster Recovery

Enterprise-grade backup procedures across all critical systems. Daily automated backups for critical production systems. Continuous backups for productivity and collaboration platforms. Documented RTO/RPO. Quarterly testing: File recovery, email restoration, code repository validation. Annual testing: Full database restoration, infrastructure recovery, end-to-end disaster scenarios. Documented procedures for accidental deletion, ransomware, cloud outages, and key personnel unavailability.

### 4.7 People & Training

Mandatory annual security awareness training for all employees covering threats, phishing, incident reporting, password hygiene, GDPR fundamentals. IBM Gold Partner: Annual external integrity certification covering financial compliance, antitrust, data protection, respectful workplace. Technical staff: Secure coding, vulnerability management, incident response. Management: Data ethics leadership via QBLearning/Edutech Nordic. Training completion tracked quarterly, annual recertification required.

### 4.8 Supplier Management

All Category A (critical) suppliers must hold SOC 2 Type II or ISO 27001 certification, notify incidents within 24 hours, undergo quarterly security reviews, maintain documented backup/recovery procedures, provide annual audit reports. Category B suppliers: Annual reviews, ISO/SOC preferred. Platform partners maintain: SOC 2/ISO 27001 certification, 24/7 enterprise support, published security documentation, regular updates, incident disclosure procedures, DPAs with appropriate safeguards.

# 5. Compliance & Certifications

## 5.1 Regulatory Compliance

**NIS2 Directive (Directive (EU) 2022/2555)**

IMG Play is fully compliant with the EU NIS2 Directive, implementing all 10 required cybersecurity measures under Article 21.

**GDPR (General Data Protection Regulation)**

Complete compliance with EU GDPR including Articles 5, 24, 25, 28, 30, 32, 33, and 35. Full ROPA (Record of Processing Activities) maintained. 72-hour breach notification procedures.

**EU AI Act (Regulation 2024/1689)**

Limited Risk AI systems with transparency obligations. No High-Risk or Unacceptable Risk systems deployed. Human oversight mandatory for all AI-assisted processes. AI System Inventory maintained.

## 5.2 Certifications & Partnerships

Active Certifications:

- ✅ IBM Gold Partner (certified) - With annual integrity certification
- ✅ NIS2 Directive compliant - All 10 Article 21 requirements
- ✅ GDPR compliant - Complete framework implemented
- ✅ SOC 1 & SOC 2 Type 2 audited infrastructure (SSAE-18 standards)
- ✅ ISO 27001 certified infrastructure (all critical suppliers)

Memberships & Recognition:

- ✅ UN Global Compact Network Denmark (member since 2020) - Active support of Ten Principles
- ✅ ESG and CSRD reporting alignment for sustainable business practices
- ✅ Entertainment industry security validation (Hollywood studio audits passed)
- ✅ Dun & Bradstreet AA Diploma (October 2025) - High creditworthiness (top 2% in Denmark)

## 6. Your Data, Your Control

### 6.1 What We Process

**IMG Play is a technology integrator, not a processor of end-user content.**

We ONLY process:

- Your company contact information (for business relationship management)
- Technical support tickets (30-day retention in secure ticketing system)
- System logs for troubleshooting (90-day retention)
- Account identifiers from platforms (for integration configuration only)
- Workflow metadata (project management, deployment logs)

We do NOT process:

- Your end-user content (media files, documents, data)
- Your customer personal data or analytics
- Any data within your enterprise platforms
- Payment information from end users
- Viewer information or usage analytics

### 6.2 Your Content Security

Your content remains entirely within your chosen enterprise platforms. IMG Play does not have access to your content or end-user data. Our role is strictly limited to platform configuration, integration, and technical support.

### 6.3 Data Location & Transfers

Primary processing: European Union (Denmark). Cloud storage: EU regions preferred. International transfers only where suppliers provide adequate safeguards via Standard Contractual Clauses (SCCs) or EU-US Data Privacy Framework compliance.

# 7. Governance & Oversight

## 7.1 Leadership Accountability

**CEO Responsibility (NIS2 Article 20)**

Karsten Vandrup Westh, CEO, has personal accountability for IMG Play's information security program, as required by NIS2 Article 20. This includes board-level approval of security measures, quarterly management reviews, annual policy reviews, mandatory training, and final approval authority for all security investments.

## 7.2 Policy Framework

Our security program is governed by 15 comprehensive operational policies covering IT security, encryption standards, network security, HR security, asset management, business continuity, supplier management, security testing, development processes, incident handling, vulnerability management, GDPR compliance, data processing, training, and CEO accountability.

All policies are reviewed annually (every November) and updated as needed.

**Next comprehensive review:** November 2026

# 8. Continuous Improvement & Sustainability

Security is not a destination but a continuous journey. We continuously improve through regular assessments, industry best practice adoption, threat intelligence monitoring, employee training, lessons learned from incidents, customer feedback, and transparent project documentation.

## 8.1 Sustainability (UN Global Compact Member)

As a UN Global Compact Network Denmark member since 2020, we actively support the Ten Principles on human rights, labor, environment, and anti-corruption. We align with ESG reporting principles, prepare for CSRD compliance, and contribute to Sustainable Development Goals (SDGs) through responsible business practices.

## 9. Reporting Security Concerns

We take all security concerns seriously and encourage responsible disclosure.

**Report Security Issues:**

📧 security@imgplay.com

📞 +45 7027 3060 (business hours)

Emergency support available 24/7 via technical management

**For Data Protection Inquiries:**

📧 privacy@imgplay.com

Data Protection Officer: Karsten Vandrup Westh, Chief Executive Officer

### Our Commitment to Reporters:

- ✅ Acknowledge your report within 24 hours
- ✅ Investigate all reported issues thoroughly
- ✅ Keep you informed of our response and remediation
- ✅ Recognize and appreciate responsible disclosure
- ✅ No legal action against good-faith security researchers

## 10. Contact & Related Information

### 10.1 Contact Us

IMG Play ApS

Rahbeks Allé 21

1801 Frederiksberg

Denmark

📞 +45 7027 3060

📧 info@imgplay.com

🌐 www.imgplay.com

Security Contact: security@imgplay.com

Privacy Contact: privacy@imgplay.com

CVR: 37000728

### 10.2 Related Documentation

Public Documentation:

- Security Summary - Executive overview of our security program
- Privacy Policy - How we handle personal data
- Data Processing Information - Our role as data processor/integrator

For access to detailed internal policies, please contact security@imgplay.com

## 11. Revision History

| Version | Date | Changes | Approved By |
|---|---|---|---|
| **1.0** | July 2025 | Initial release | CEO |
| **2.0** | November 26, 2025 | Added industry recognition, expanded training, sustainability | CEO |
| **2.1** | November 26, 2025 | Removed specific tool/platform names, broader technology focus, enhanced for external publication | CEO |
| **2.2** | December 12, 2025 | Added Dun & Bradstreet AA Diploma financial rating | CEO |

**Next Review:** November 2026

## Approval

Name: Karsten Vandrup Westh

Title: Chief Executive Officer

Date: ____12. december 2025_____

Signature: 

— End of Information Security Statement —