IMG Play ApS

SECURITY SUMMARY

Document Title:	Security Summary
Version:	2.3
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. Overview

IMG Play ApS is a Nordic technology consultancy and systems integrator specializing in enterprise media workflows, secure data transfers, and cloud-based infrastructure solutions.

Our security model is built on NIS2, EU AI Act, ISO 27001, SOC 2, GDPR, and enterprise platform standards. Security, compliance, and ethical operations are integrated into everything we deliver.

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

We maintain a complete security, governance, and compliance framework covering:

- Risk management and continuous risk assessment
- Incident handling with defined escalation procedures
- Business continuity and disaster recovery
- Secure development lifecycle (SDLC)
- Supply chain security assurance
- Encryption and identity management
- Cybersecurity training and awareness
- Access controls and monitoring
- Vulnerability management
- AI governance and data ethics

2. Governance & Compliance Framework

IMG Play maintains a complete suite of policies and procedures fully aligned with NIS2 Article 21, EU AI Act, D-mark certification requirements, and industry best practices.

2.1 Certifications & Partnerships

Active Certifications:

✅ IBM Gold Partner (certified) - Annual integrity certification and training for all employees
✅ NIS2 Directive compliant - All 10 Article 21 requirements implemented
✅ GDPR compliant - Complete framework with ROPA and Personal Data Policy

✅ SOC 1 & SOC 2 Type 2 audited infrastructure (SSAE-18 standards)
✅ ISO 27001 certified infrastructure via all critical platform partners
✅ Dun & Bradstreet AA Diploma (October 2025) - High creditworthiness (top 2% in Denmark)

2.2 Policy Framework

Our comprehensive framework includes 15 operational policies:

1. IT Security Policy - Master security framework
2. Encryption Standards (Appendix A) - MFA enforcement matrix for 9 systems
3. Network Security & Zero Trust (Appendix B) - 94 paragraphs covering five security pillars
4. HR Security Policy (Appendix C) - Onboarding/offboarding with 1-hour termination SLA
5. Asset Register - Complete inventory with 4-tier classification
6. IT Contingency Plan - 13-system backup matrix with RTO/RPO
7. Supplier Policy - NIS2 Article 21 compliant supply chain security
8. Security Testing Policy - 48-hour critical vulnerability SLA
9. Development Process - 118-paragraph secure SDLC
10. Incident Handling Process - NIS2 24/72-hour timelines, P1-P4 classification
11. Vulnerability Management Procedure - Complete lifecycle management
12. Personal Data Policy - 88-paragraph GDPR framework
13. ROPA (Record of Processing Activities) - GDPR Article 30
14. Training and Awareness - IBM Gold Partner + data ethics training
15. NIS2 Compliance Summary - CEO - Executive accountability framework

All governance documents are reviewed annually and whenever significant system changes occur.

2.3 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 security reviews with management
- Annual comprehensive policy review
- Mandatory cybersecurity training completion
- Personal liability for compliance and security posture

2.4 Corporate Social Responsibility & UN Global Compact

UN Global Compact Network Denmark Membership

Since 2020, IMG Play has been a proud member of the UN Global Compact Network Denmark, the world's largest corporate sustainability initiative. This membership reflects our commitment to responsible business practices and sustainable development.

Our Commitment to the Ten Principles

IMG Play actively supports and implements the UN Global Compact Ten Principles across four key areas:

Human Rights

Principle 1: Support and respect the protection of internationally proclaimed human rights
Principle 2: Ensure we are not complicit in human rights abuses

Implementation: Our Responsible AI Policy ensures technology is used ethically and respects human dignity. We prohibit AI systems for social scoring, manipulation, or profiling. All employees receive annual integrity training covering respect, inclusion, and harassment-free workplace standards.

Labour

Principle 3: Uphold freedom of association and effective recognition of collective bargaining
Principle 4: Eliminate all forms of forced and compulsory labour
Principle 5: Abolish child labour
Principle 6: Eliminate discrimination in employment and occupation

Implementation: IMG Play maintains fair employment practices with transparent contracts, competitive compensation, and professional development opportunities. Our IBM Gold Partner integrity training covers anti-discrimination, workplace equality, and respectful collaboration. We conduct annual access reviews and maintain documented HR security procedures ensuring fair treatment throughout the employee lifecycle.

Environment

Principle 7: Support a precautionary approach to environmental challenges
Principle 8: Undertake initiatives to promote greater environmental responsibility
Principle 9: Encourage development and diffusion of environmentally friendly technologies

Implementation: As a cloud-native integrator, IMG Play leverages ISO 27001 and SOC 2 certified infrastructure providers who invest heavily in renewable energy and energy-efficient data centers. We minimize physical hardware, operate paperless where possible, and partner with enterprise platforms committed to environmental sustainability. Our secure file transfer solutions reduce the need for physical media shipments.

Anti-Corruption

Principle 10: Work against corruption in all its forms, including extortion and bribery

Implementation: IMG Play employees complete annual IBM Gold Partner integrity certification covering compliance with financial laws, anti-bribery standards, and antitrust regulations. We maintain transparent financial systems, documented procurement procedures, and clear governance oversight. Our Supplier Policy requires ethical business practices from all partners.

ESG & CSRD Alignment

Beyond UN Global Compact, IMG Play aligns with Environmental, Social, and Governance (ESG) principles and prepares for Corporate Sustainability Reporting Directive (CSRD) compliance:

- Environmental: Cloud-native operations, minimal physical footprint, certified green infrastructure partners
- Social: Fair employment, diversity and inclusion, data ethics leadership, community engagement
- Governance: CEO accountability (NIS2 Article 20), board oversight, transparent reporting, ethical AI practices

Contribution to Sustainable Development Goals (SDGs)

IMG Play's operations contribute to multiple UN SDGs:

- SDG 8 (Decent Work and Economic Growth): Fair employment, professional development, safe working conditions
- SDG 9 (Industry, Innovation and Infrastructure): Technology innovation, secure infrastructure, digital transformation
- SDG 12 (Responsible Consumption and Production): Cloud efficiency, paperless operations, minimal waste
- SDG 13 (Climate Action): Low-carbon digital services, green infrastructure partnerships

- SDG 16 (Peace, Justice and Strong Institutions): Transparent governance, anti-corruption, data protection

Communication on Progress
As a UN Global Compact participant, IMG Play commits to annual Communication on Progress (CoP) reporting, transparently sharing our CSR activities, progress, and challenges with stakeholders.

External Verification
Our commitment to the UN Global Compact Ten Principles is externally verified through:

- IBM Gold Partner annual integrity certification (covers principles 1, 2, 4, 5, 6, 10)
- ISO 27001 and SOC 2 certified infrastructure (environmental responsibility, governance)
- GDPR compliance and D-mark certification pursuit (human rights, data ethics)
- NIS2 Article 20 CEO accountability (governance and oversight)
- Hollywood studio security audits (responsible business practices)

3. Cloud & Platform Security

IMG Play exclusively uses ISO 27001 and/or SOC 2 Type II certified infrastructure and platform providers. All critical suppliers (Category A) are fully audited annually.

3.1 Infrastructure Partners

Our infrastructure and platform partners maintain enterprise-grade security certifications:

Category	Service Type	Security Standards
Cloud Hosting (Category A)	PaaS/IaaS	SOC 2 Type II, ISO 27001
Enterprise Platforms (Category A)	Media delivery & workflows	SOC 2 Type II, ISO 27001
Productivity Tools (Category B)	Collaboration & storage	SOC 2, ISO 27001, GDPR certified

3.2 Supplier Assurance

We maintain:

- 24/7 supplier status monitoring

- Quarterly supplier security reviews for Category A partners
- Annual reviews for Category B partners
- DPAs, sub-processor lists, and SLA verification
- ISO 27001 / SOC 2 certificate validation (annual)
- 24-hour incident disclosure requirement for Category A
- Cascading risk assessment procedures per NIS2 Article 21

4. Encryption & Identity Security

Zero Trust identity model with MFA mandatory across all 9 IMG Play-controlled systems. AES-256 encryption at rest, TLS 1.3 in transit. All credentials stored in 1Password Business. Role-based access control with quarterly reviews. 1-hour offboarding SLA for access revocation.

5. Secure Development & Operations

Automated security: GitHub automated dependency vulnerability scanning (daily dependency scanning) (SAST), Secret Scanning, Sentry.io runtime monitoring (90-day retention). Manual controls: Code review mandatory, protected branches, environment variable secrets only. CI/CD security checks on every commit.

6. Data Protection & GDPR

Complete ROPA (Record of Processing Activities) and Personal Data Policy per GDPR Article 30. IMG Play processes minimal personal data: company contacts, support tickets (30-day retention), system logs (90-day retention). 72-hour breach notification procedures. Quarterly GDPR compliance reviews. No customer end-user data stored on IMG Play systems.

7. AI Governance & Ethics

EU AI Act compliant - Limited Risk systems only. All AI usage documented in AI System Inventory. Human oversight mandatory. No High-Risk or Unacceptable Risk systems. Prohibited practices: social scoring, manipulation, real-time biometric ID, emotion recognition, predictive policing. Data ethics leadership training via QBLearning/Edutech Nordic. Responsible AI Policy aligned with OECD principles.

8. Training & Professional Development

IBM Gold Partner: Annual integrity certification for all employees covering financial compliance, antitrust, data protection, respectful workplace. Security awareness: Mandatory annual training, phishing recognition, incident reporting. Technical staff: Secure coding, vulnerability management. Management: Data ethics leadership (QBLearning/Edutech Nordic), NIS2 compliance, board reporting.

9. Business Continuity & Disaster Recovery

Complete 13-system backup matrix with documented RTO/RPO. Daily automated backups for critical systems. Quarterly testing (Dropbox, Office 365, GitHub). Annual disaster recovery drills. Documented procedures for ransomware, outages, key personnel unavailability. Supplier-integrated DR options. All tests documented in Backup Test Log.

10. Vulnerability Management

Remediation SLAs: Critical (48 hours), High (7 days), Medium (30 days), Low (90 days). GitHub automated dependency vulnerability scanning daily scanning. CVSS 3.1 scoring. Weekly vulnerability reviews by Technical Manager and Senior Developer. Target: 100% critical remediation within 48 hours. All remediation tracked in Vulnerability Log. CEO notification for all critical (P1) vulnerabilities.

11. Incident Response

P1-P4 severity classification. Response times: P1 <1 hour, P2 <4 hours, P3 <24 hours, P4 <72 hours. CEO notification immediate for P1 incidents. NIS2 regulatory timelines: 24-hour early warning to CFCS, 72-hour full notification, 1-month final report. GDPR: 72-hour breach notification. 7-step workflow: Detection → Assessment → Notification → Containment → Eradication → Recovery → Closure. Post-incident review within 7 days.

12. Continuous Improvement & Quality

Security and quality are not static targets but continuous journeys. IMG Play is committed to:

- Upholding the highest compliance and security standards
- Continuously improving through collaboration and customer feedback
- Leading responsibly in delivering advanced technology solutions
- Transparent documentation and accountability (teamwork.com project tracking)
- Regular security assessments and penetration testing
- Industry best practice adoption and threat intelligence monitoring
- Technology updates and enhancements based on emerging threats
- Lessons learned documentation from security incidents
- Annual comprehensive policy review (every November)

Next comprehensive review: November 2026

13. Contact & Escalation

For security-related matters:

Security Incidents & Vulnerabilities: security@imgplay.com

Data Protection Inquiries: privacy@imgplay.com

General Contact: contact@imgplay.com

Emergency (24/7): +45 7027 3060

IMG Play ApS
Rahbeks Allé 21
1801 Frederiksberg, Denmark
CVR: 37000728
www.imgplay.com

14. Revision History

Version	Date	Changes	Approved By
1.0	July 2025	Initial release	CEO
2.0	October 2025	NIS2 framework integration	CEO
2.1	November 26, 2025	Added Hollywood audits, UN Global Compact, IBM details, D-mark status	CEO
2.2	November 26, 2025	Expanded CSR/UN Global Compact section, less vendor-specific, broader technology focus	CEO
2.3	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 Security Summary —

For detailed policies, please contact security@imgplay.com