Information Protection Policy

Document Type	Policy
Document Status	RELEASED
Classification	Public - Redacted Copy
Owner	C Christian Senk
Version	8.0
Date	August 31, 2026
Approved By	J James Brooke
Purpose	This Policy applies globally to all Mapp Digital (“Mapp”) entities and to all information assets, systems (including AI systems), processes, and technologies managed or controlled by Mapp, including third-party and cloud-based environments. It establishes Mapp's commitment to information security (including operational resilience and business continuity), data protection, and responsible AI governance through robust, certifiable controls that ensure compliance with legal, regulatory, and contractual obligations.
Target Group	All Mapp Employees (incl. Contractors); on demand: Business Partners, Customers, and Resellers

Why This Policy Exists

Our Commitment

How We Deliver

- One Management System
- Clear Accountability

The Rules

- Principles
  - 🔒 Keeping Information Secure
  - 🛡️ Protecting Personal Data
  - 🤖 Using AI Responsibly
- High-Level Requirements
- Supplementary Policies

What We Ask of You
- 📖 Know Your Standards
- 🚨 Report Incidents Immediately
- 📨 Forward Data Subject Requests
- 🚦 Planning a Project or Big Change? Involve Us Early
- 🙋 Need an Exception? Ask Us

Compliance and Disciplinary Consequences

Glossary

> 🧭 **How to read this Policy:** It states Mapp's promise (*Our Commitment*), how we deliver it (*How We Deliver*), the binding rules (*The Rules*), and what that means for you personally (*What We Ask of You*). Your day-to-day rules live in the 🔐 Information Protection Standard. Unfamiliar terms are explained in the **Glossary** at the end.

Why This Policy Exists

Our customers entrust Mapp with their most valuable asset: their data. Safeguarding it, together with the personal data of everyone we work with, is the foundation of that trust, and the reason this Policy exists.

Security, data protection, and responsible AI are not three separate topics. The same information flows through our systems (security), is about real people (privacy), and is increasingly processed by intelligent tools (AI). A weakness in one is a weakness in all. That is why Mapp runs one integrated protection programme: one management system, one control framework, one line of accountability.

This Policy applies globally to all Mapp entities and to all information assets, systems (including AI systems), processes, and technologies managed or controlled by Mapp, including third-party and cloud-based environments.

Our Commitment

At Mapp, three things matter equally: keeping our information safe, protecting people's personal data, and using AI responsibly. Operational resilience and business continuity are part of the first: information that is not available when the business needs it is not protected. Every one of us plays a part. Here is what we promise:

- **One system, always improving:** We manage security, privacy, and AI in one management system, certified to ISO 27001 and aligned with ISO 27017 and 27018, and we make it better every year. Whatever we do with information, we do it ethically and fairly.
- **Empowered people:** Everyone at Mapp, leaders included, is trusted and expected to make thoughtful decisions, speak up when something feels wrong, and take responsibility for protecting information, privacy, and responsible AI use.
- **Protected and resilient:** We protect our own and our customers' information with strong, state-of-the-art defences that match the actual risk, and we are prepared for the day something breaks so we can keep critical operations running.

- **Privacy first:** We design privacy in from day one, collect and keep personal data only for clear, legitimate reasons and never longer than necessary, and respect people's rights over their own data.
- **Humans in charge:** We maintain oversight of what our AI does, keep a named person accountable for every AI system, weigh how risky it is, and never let AI make important decisions about people on its own.
- **Compliance, non-negotiable:** We know which security, privacy, and AI laws apply to us, such as the GDPR and the EU AI Act. We treat them as our minimum standard, and we can demonstrate compliance whenever required.

Standing behind this promise are those accountable for delivering it:

@James Brooke	@Eric Lubow	@Christian Senk
Chief Executive Officer	Chief Product & Technology Officer	Chief Security & Privacy Officer

---

How We Deliver

One Management System

One risk method, one improvement cycle, and one unified control framework (the Mapp Control Framework, MCF) drive security, privacy, AI governance, and reliable service delivery through our Information Security Management System (ISMS). We call this integrated system the **Information Protection Program**: both terms refer to the same thing throughout this Policy and its supplementary documents, with ISMS as the technical, certification-facing name. We translate our core principles into measurable, annually reviewed objectives with clear accountability. The 📘 ISMS Handbook details how this integrated system is planned, operated, and improved.

Clear Accountability

Accountability runs in one unbroken line from the CEO to every employee, and every role covers security, data protection, and AI governance together. There are no separate silos.

- **Senior Leadership Team:** Led by the Chief Executive Officer (CEO), it holds ultimate accountability for information security, data protection, AI governance, operational resilience, risk, and compliance. Our CEO @James Brooke keeps business objectives and information protection aligned and takes final decisions in the organisation's best interests; our Chief Product & Technology Officer @Eric Lubow sponsors the ISMS at executive level and ensures it is fully integrated into product and technology operations.
- **Technology Leadership Team (TLT):** Chaired by the Chief Product & Technology Officer, it drives Mapp's technology strategy and embeds security, data protection, responsible AI, and operational resilience in all systems and services.
- **Chief Security & Privacy Officer (CSPO):** Our CSPO @Christian Senk develops, operates, and continually improves the Information Protection Program (our ISMS), with the authority to define and enforce security, data protection, and AI governance standards across all Mapp entities. The **Data Protection Officer (DPO)** role sits with the CSPO, keeping data protection and information security closely aligned; the DPO oversees compliance with the EU GDPR, UK GDPR, and other applicable privacy laws.

- **Protect Team:** A virtual, cross-functional team supporting the CSPO. It coordinates and enforces the Information Protection Program across departments, in line with the 📘 ISMS Handbook.
- **Legal Team:** Identifies and interprets legal, regulatory, and contractual obligations, assists with legal assessments where needed, and keeps contracts, required safeguards, authority communications, insurance, and the whistleblower channel aligned with Mapp's protection requirements.
- **Managers and specialist roles:** Team leads and service owners keep their areas compliant, meet agreed service levels, and involve the Protect Team early when changes may affect security, privacy, or resilience. Technical, service-facing, Information Owner, and Asset Owner roles implement the relevant controls in day-to-day work.
- **Every employee:** Follows Mapp's information protection policies, covering security, data protection, and responsible AI use, and reports violations, weaknesses, and improvement ideas (see What We Ask of You).
- **Third parties and business partners:** Meet Mapp's security, data protection, and AI requirements as specified in their contracts.
- **Customers and resellers:** Follow the Acceptable Use Policy referenced in the Mapp Cloud Service Terms and manage their own data and service access, while Mapp secures the underlying cloud infrastructure and services.

The Rules

Our rules work in three layers:

1. **Principles:** the states that are always true at Mapp, one set per pillar of Our Commitment.
2. **High-Level Requirements:** the shared control framework that enforces all three pillars at once.
3. **Supplementary Policies:** the standards that turn principles and controls into concrete rules for each audience.

Throughout all of them, the wording tells you how binding a rule is:

- **Must:** mandatory; required for compliance.
- **Should:** recommended good practice; follow it unless there is a good reason not to, and be prepared to explain significant deviations.
- **May:** optional or permitted when appropriate.
- **Must not / May not:** prohibited under this Policy or applicable law.
- **Should not:** discouraged unless clearly justified.

If no such word is used, the requirement is mandatory.

▼ Where this convention is defined and how far it reaches

This wording convention follows the central definition in the 📘 ISMS Handbook (Policy Language) and applies to **every document of the Information Protection Program**: this Policy and all Supplementary Policies and Standards listed below. A *must* in a supporting Standard is exactly as binding for its target group as a *must* in this Policy.

Principles

These principles bind everyone and everything Mapp does. They are deliberately written as states, not commands: each one describes what is true at Mapp when we work as intended. The High-Level Requirements and the supplementary policies further below carry the binding language that keeps these states true, as concrete, audience-specific rules.

🔒 Keeping Information Secure

- **Confidentiality, integrity, and availability:** Information is protected across its whole lifecycle: only authorised people can access it, it stays accurate and complete, and it is available when the business needs it.
- **State of the art, applied with judgement:** Controls match the actual risk and reflect the state of the art: layered defences where they protect, no unnecessary complexity where it adds nothing.
- **Least privilege:** Access to information and systems is granted based on business need, limited to what a person, system, or AI agent reasonably requires, and reviewed when that need changes.
- **Secure by design:** Systems, applications, and supplier relationships have security built in from the start, not bolted on later.
- **Resilience by preparation:** Critical operations survive disruption: we plan, back up, and rehearse recovery before we need it, and we detect and respond to incidents fast.

🛡️ Protecting Personal Data

- **Lawfulness and consent:** Personal data is processed only on a valid legal basis: consent, legitimate interest, or performance of a contract. Where consent is relied upon, it is informed, unambiguous, and freely given, through a clear, easily understandable mechanism offered at (or as soon as practicable after) collection.
- **Privacy by Design and by Default:** Systems and procedures minimise the personal data processed and limit access to what is necessary; defaults favour data subject anonymity and low data linkability.
- **Transparency:** Data subjects are informed how Mapp processes their data (use, disclosure, retention, disposal, and how to contact Mapp and its Data Protection Officer) through the applicable privacy notices, including major changes to data handling.
- **Shared responsibility in customer processing:** Mapp processes Customer Data as Processor, under a written contract and only on the instructions of the customer as Controller. Customers remain responsible for lawful processing within the Mapp Cloud Software Services (including necessary consents), for data minimisation, and for enabling data subjects to exercise their rights within the services.
- **Data quality:** Personal data is accurate, complete, and current, supported by proportionate input and output controls.

🤖 Using AI Responsibly

- **Enthusiasm with guardrails:** Mapp embraces AI and aims to be an early adopter: we actively explore and use AI to work smarter, build better products, and serve customers faster, always within the guardrails of this Policy and its standards, and never at the expense of security, privacy, or customer trust.
- **No high-risk or prohibited uses:** Mapp does not build or use AI for purposes that are prohibited or classified as high-risk under applicable AI regulation, for example social scoring, manipulative techniques, emotion recognition in the workplace, or decisions with legal or similarly significant effect on individuals made by AI alone.

- **Human oversight and accountability:** A named person is accountable for every AI system, and AI never makes important decisions about people on its own. All AI built or used at Mapp is inventoried and risk-assessed before and during adoption.

High-Level Requirements

One control framework carries all three pillars. The fourteen requirement domains below are the mandatory backbone of the Information Protection Program; most serve security, data protection, and AI governance at once (`Legal Compliance`, for example, carries the privacy obligations, and `Application & Interface` carries the AI controls, from agent guardrails to human oversight). Each domain is enforced through the referenced controls; their names and detailed descriptions are maintained in the Mapp Control Framework (MCF) catalogue.

- **Governance & Risk:** A comprehensive management system must be established and maintained to guide organisational practices, mitigate information risks, and ensure continuous improvement across information security, data protection, AI governance and operational resilience. `MCF-01.01–08`
- **Legal Compliance:** All applicable legal, regulatory, and contractual obligations must be identified, documented, and continuously monitored to ensure compliance and accountability. `MCF-02.01–05`
- **Customer:** Customer-related services and processes must be managed throughout the service lifecycle to deliver agreed service levels, ensure operational resilience, and safeguard customer assets. `MCF-03.01–03`
- **People & Workspace:** A competent workforce and secure workplace must be maintained to protect assets, ensure operational efficiency, and uphold security standards. `MCF-04.01–06`
- **User Devices:** All end-user devices must be protected by appropriate security controls to prevent unauthorised access or data loss. `MCF-05.01`
- **Information Protection:** Information must be protected throughout its lifecycle, ensuring confidentiality, integrity, and availability aligned with business needs. `MCF-06.01–04`
- **Identity & Access:** Access to information and systems must be controlled to prevent unauthorised use while ensuring appropriate access for authorised users. `MCF-07.01–03`
- **System & Network:** System and network reliability, security, and performance must be maintained through consistent management, monitoring, and improvement. `MCF-08.01–09`
- **Application & Interface:** Applications, interfaces, and AI systems must be designed, developed, and maintained securely to ensure reliability, protect data interactions, and keep AI behaviour within controlled boundaries under human oversight. `MCF-09.01–05`
- **Data Center:** Physical infrastructure must be protected to ensure the integrity, availability, and performance of critical systems. `MCF-10.01–02`
- **Physical Media:** Physical media must be managed securely during handling, storage, transport, and disposal to prevent unauthorised access. `MCF-11.01`
- **Supply Chain:** Supplier relationships must be managed to ensure reliability, compliance, and effective risk mitigation throughout the supply chain. `MCF-12.01–02`
- **Incident Response:** Security and privacy incidents must be promptly detected, investigated, and resolved to minimise impact and drive continuous improvement. `MCF-13.01`
- **Resilience:** Critical operations and services must remain available through proactive planning, redundancy, and recovery measures that minimise disruption. `MCF-14.01–03`

Supplementary Policies

The following topic-specific policies and standards turn the principles above into concrete rules for each audience. They are an integral part of the Information Protection Program and equally binding wherever they apply. The starting point for every employee is the 🔐 Information Protection Standard.

Find your standard:

- **Everyone at Mapp:** Start with the 🔐 Information Protection Standard and the applicable 🤫 Employee Confidentiality Policy or 🤐 Contractor Confidentiality Policy.
- **Employees building AI tools or agentic workflows:** Use the 🤖 AI Builder Standard.
- **Managers and Service Owners:** Use the 💼 Business Application Security Standard for business applications and the 🤝 Third Party Provider Management Standard when suppliers are involved.
- **Product, Engineering, QA, Infrastructure, and DevOps:** Use the 🔒 Mapp Cloud Application Security Standard and ⚙️ Mapp Cloud Platform Operations Security Standard.
- **Customer-facing teams:** Use the ☁️ Mapp Cloud Services Security Standard when handling customer systems, customer data, or support and service delivery.
- **IT Administrators (Corporate Systems):** Use the 🖥️ Corporate Systems Security Standard for internal IT infrastructure and corporate systems.
- **HR and Office Management:** Use the 👥 People Security Standard and 🏢 Office Security Standard for workforce, employment, workplace, and office-security topics.
- **Protect, DPO, and project teams:** Use the 🔏 Information Compliance and Data Protection Standard for processing accountability, data subject rights, transfers, and authority or disclosure handling.
- **Management and Protect Team:** Use the 🆘 Emergency Handbook when an incident escalates to an emergency or crisis, and the 🛟 Business Continuity Policy for keeping mission-critical functions resilient and recoverable.
- **Protect Team:** Use the 🚨 Information Security Incident Management Standard for identifying, handling, and resolving security incidents, and the 📘 ISMS Handbook for operating, assessing, and improving the Information Protection Program.

Document	Purpose	Focus	Target Group
🔐 *Information Protection Standard*	Establishes mandatory rules on IT and AI usage, information security and privacy for employees.	`People & Workspace` `Information Protection`	All Employees
🤫 *Employee Confidentiality Policy*	Defines every employee's binding obligation to protect company information.	`People & Workspace` `Information Protection`	All Employees
🤐 *Contractor Confidentiality Policy*	Defines every contractor's binding obligation to protect company information.	`People & Workspace` `Supply Chain`	All Contractors
🤖 *AI Builder Standard*	Defines guardrails for self-developed AI tools and agentic workflows built by employees.	`Application & Interface`	All Employees building AI tools or agentic workflows

Document	Purpose	Focus	Target Group
💼 *Business Application Security Standard*	Establishes rules for the secure and compliant setup and handling of business applications.	`Application & Interface`	Managing Roles (Service Owners)
🤝 *Third Party Provider Management Standard*	Governs vendor management to ensure security and compliance.	`Supply Chain` `Customer`	Legal Team, Protect Team, Managing Roles (Service Owners)
🔒 *Mapp Cloud Application Security Standard*	Defines security, data protection, and compliance standards for Mapp Cloud applications.	`Customer` `Application & Interface`	Technical Roles (Product Managers, Software Developers, Quality Assurance)
⚙️ *Mapp Cloud Platform Operations Security Standard*	Defines standards for the secure operations of the Mapp Cloud platform.	`Customer` `Identity & Access` `System & Network` `Data Center` `Physical Media` `Incident Response` `Resilience`	Technical Roles (Administrators / Infrastructure & DevOps)
☁️ *Mapp Cloud Services Security Standard*	Outlines protocols for securing Mapp Cloud customer systems and data.	`Customer` `Information Protection`	Service Roles (Professional Services, Account Management and Customer Success, Technical Support)
🖥️ *Corporate Systems Security Standard*	Sets responsibilities and standards for managing internal IT infrastructure and corporate systems.	`User Devices` `Identity & Access` `System & Network` `Data Center` `Incident Response` `Resilience`	Technical Roles (Corporate Systems)
👥 *People Security Standard*	Ensures employees understand and fulfil their security responsibilities and employment records are effectively protected.	`People & Workspace`	Human Resources

Document	Purpose	Focus	Target Group
🏢 *Office Security Standard*	Defines operational and physical security measures for office spaces.	`People & Workspace` `Data Center` `Physical Media`	Human Resources, Office Management
🔏 *Information Compliance and Data Protection Standard*	Defines how data protection and information compliance are operationalised: processing accountability, international transfers, data subject rights, and authority and disclosure handling.	`Legal Compliance`	Legal Team, Protect Team (DPO); consulted by Project & Service Teams
🆘 *Emergency Handbook*	Provides the emergency and crisis response organisation, declaration criteria, and communication procedures for severe incidents.	`Incident Response` `Resilience`	Protect Team, SLT, TLT
🛟 *Business Continuity Policy*	Outlines our policy on business continuity, aimed at minimising disruptions and ensuring the resilience of mission-critical functions to swiftly recover from incidents.	`Resilience`	Management, Protect Team
🚨 *Information Security Incident Management Standard*	Describes how to identify, handle, and resolve security incidents.	`Incident Response`	Protect Team
📘 *ISMS Handbook*	Outlines the framework and processes for planning, operating, and improving the Information Protection Program, addressing requirements related to business, risk, and compliance.	`Governance & Risk`	Protect Team

What We Ask of You

Policies don't protect anything; people do. Whatever your role, five things apply to you personally. (For partners, customers, and resellers, the equivalent obligations live in your contract and the Acceptable Use Policy.)

📖 Know Your Standards

Follow the standards for your role. For everyone, that starts with the 🔐 Information Protection Standard; the table above shows which further standards apply to you. If anything is unclear, ask the Protect Team. Asking early is always cheaper than fixing later.

🚨 Report Incidents Immediately

Report every security, data protection, or AI-related incident promptly, even if you only suspect one. When in doubt, report: a false alarm costs minutes, an unreported incident can cost far more. Typical examples include phishing, compromised credentials, unauthorised system or physical access, device loss or theft, and malware.

Where to report:

- Internal IT-related security issues: the Helpdesk Team or the Jira Service Desk.
- Broader security and data protection concerns: the Protect Team or a Protect Ticket.
- Non-security IT issues: the responsible System Administrator.
- Customers report incidents via our Technical Support Portal.

When reporting, describe the incident, its scope, and its urgency, and keep details confidential: share them only with those who need to know. The full process is described in the 🚨 Information Security Incident Management Standard.

> 🕊️ **Whistleblowing:** To report violations or misconduct confidentially, use the designated Whistleblower Channel. Reports can be made anonymously; the reporter's identity is protected while the claim is thoroughly investigated.

📨 Forward Data Subject Requests

If you receive a request from a data subject concerning their personal data rights (e.g., access, correction, or deletion of personal data), forward it promptly to the Privacy Inbox or the Data Protection Officer and do not answer it yourself. The Protect Team processes the request and ensures a timely and formally accurate response.

🚦 Planning a Project or Big Change? Involve Us Early

Every significant project or business change must be assessed for its impact on security, privacy, and compliance **before go-live**. If you own such an initiative, engage the Protect Team early in the planning phase, especially when critical data or services are involved, standard controls don't fit, or new technology is used. Triage, assessment, and decision follow the process in the 📘 ISMS Handbook (Project Risk and Business Changes); the initiative cannot go live until all Critical and High risks have an approved treatment plan.

🙋 Need an Exception? Ask Us

Sometimes a rule genuinely doesn't fit your situation. Don't bypass it; request an exception. Contact the Protect Team or open a Protect Ticket, describing the exception, its justification, the proposed timeframe, and any mitigation measures. The Protect Team assesses the request, may require compensating controls, and reviews granted exceptions periodically.

Compliance and Disciplinary Consequences

We verify our own compliance through audits and operational reviews (scheduled, random, or ad hoc where there is justified suspicion or an imminent threat), and we review this Policy at least annually as part of the ISMS improvement cycle. Significant violations (grossly negligent or intentional) have proportionate consequences: disciplinary action up to and including termination of employment (or, for freelancers, of the cooperation), and may entail criminal or civil liability, including compensation for damages. Honest mistakes that are promptly reported are treated as learning opportunities, not misconduct.

📜 Version History

Glossary

- **AI Governance:** The way Mapp manages the use of artificial intelligence to make sure it is ethical, transparent, secure, and compliant with data protection and privacy laws.
- **AI Systems:** Software or technology that uses artificial intelligence to perform tasks such as analysis, prediction, automation, or decision-making, based on data and algorithms.
- **Availability:** Making sure that information and systems are available and usable by authorised people when they are needed.
- **Business Continuity:** The ability of Mapp to keep essential services running, or quickly restore them, after a disruption or incident.
- **Confidentiality:** Ensuring that only authorised people can see or use information.
- **Control:** A safeguard or measure put in place to reduce risk and protect information, such as a policy, technical setting, or process.
- **Data Breach:** A confirmed event where sensitive or confidential information is accessed, shared, or stolen without authorisation.
- **Data Protection:** The way personal data is handled to make sure it stays private, secure, and used only for legitimate and lawful purposes.
- **Data Subject:** A person whose personal data is collected, used, or stored by Mapp or on its behalf.
- **Information Assets:** Any data, documents, or systems that are valuable to Mapp, including customer information, employee records, financial data, and intellectual property.
- **Information Protection Program:** Mapp's integrated programme for information security, data protection, and AI governance. Another name for the ISMS: both terms refer to the same management system.
- **Information Security:** Protecting information from being accessed, changed, destroyed, or shared without authorisation, ensuring confidentiality, integrity, and availability.
- **Information Security Incident:** Any event that affects the security of information, such as unauthorised access, a data breach, malware, phishing, or physical security violations.
- **Integrity:** Keeping information accurate, complete, and trustworthy, and preventing unauthorised changes.
- **ISMS (Information Security Management System):** The management system through which Mapp plans, operates, and continually improves information security, together with data protection and AI governance; certified to ISO 27001 and described in the ISMS Handbook. Also referred to as the Information Protection Program.
- **ISO 27001:** The international standard that defines how to set up and improve an Information Security Management System (ISMS).
- **ISO 27017:** The international standard that gives specific security guidelines for cloud service providers and customers.
- **ISO 27018:** The international standard for protecting personal data in public cloud environments.
- **Management System:** A structured way to manage policies, processes, and responsibilities so that objectives are met, risks are controlled, and continual improvement is achieved.
- **Operational Resilience:** The ability to keep critical operations running through disruption and to recover them quickly. At Mapp used interchangeably with business continuity and implemented through the

Business Continuity Policy and the Emergency Handbook.

- **Personal Data:** Any information that can identify a person, such as their name, contact details, financial data, or online identifiers like IP addresses.
- **Privacy:** The right of individuals to control how their personal data is collected, used, and shared.
- **Risk Management:** The process of identifying, evaluating, and addressing risks to reduce potential harm and keep risks within acceptable levels.