Ibexa Agentic Marketing Platform

Technical & Organisational Measures for Information Security & Data Protection (TOM)

Version:	1.0
Date of version:	07/10/2026
Document owner:	Maxime Auvy (IT security - GRC Lead)
Confidentiality level:	Restricted

Change history

Date	Version	Created by	Description of change
7/10/2026	1.0	Maxime Auvy	Initial version

Table of Content

Ibexa Agentic Marketing Platform 1
Introduction 7
What is “Ibexa Agentic Marketing Platform” ? 7
Why this document? 7
Audience of the document? 7
How to use the document? 7
Information Security Management System (ISMS) 8
Organisation of information Security 8
Policies and Procedures 8
Roles and Responsibilities 8
Risk Management 9
Risk Management Methodology 9
Human Resource Security 10
Candidate selection and Screening 10
Onboarding process 10
Security awareness and continuous education 10
Offboarding process 11
Confidentiality Clause in Employments Contracts 11
Asset management 11
Asset inventory 11
Information Classification 11
Access control 12
Ibexa’s Access Control Policy 12
Ibexa’s Password Policy 12
Ibexa’s Manager Password Policy 12
Single Sign-On (SSO) 13
MFA (Multi-Factor Authentication) 14
User Creation 14
Session Timeout 14
Segregation of duty 14
Least access privilege 15
Onboarding, offboarding, change of position & periodical reviews 15
Multi-tenant and Segregation of data 15
1. Authentication and tenant identification 15
2. Tenant tagging of data 15
3. Scoped data access 16
4. Authorisation within an organisation 16
5. Background processing 16
6. File storage 16
7. AI agent access to customer knowledge 17
8. Inbound integrations (webhooks) 17

9. Verification 17
Cryptography 18
Encryption of data at rest 19
Encryption of data in transit 19
Physical and Environmental Security 19
Data processing facilities 19
Ibexa's Offices 20
Ibexa's laptops 20
Hard drive encryption 20
Antimalware protection 20
Clear screen, device locking and unattended devices 21
USB Mobile Storage Device 21
Operations Security 21
Backup Policy 21
Backup of databases 22
Backup of User Provided Content hosted by Ibexa 22
Documentation & internal files 22
Emails 23
Application code 23
DDoS and Firewalls 23
Logging & Monitoring 23
Remote access control & Intrusion Detection & Prevention 24
Communications security 24
HTTPS and SSL 24
Information Systems Acquisition Development and Maintenance 24
Secure Development Lifecycle (SDLC) 24
Features 25
Bugs 25
Customer projects 25
Teams 25
Development practices 25
Separation of environments 26
Environments accesses 26
High level architecture 26
Code review & Testing 26
Peer Code Review 27
Testing 27
Release Management 27
What is Release Management? 27
Objectives 27
Policies 28
Release Workflow 28
Lesson Learned 29
Production Data 29
Information Incident Management 29

Incident Management Procedure 29
Customer Support 29
Status Page 29
Online assistance 30
Technical vulnerabilities management and Patching policy 30
Technical vulnerabilities patching 30
Other patches and updates 30
Major version changes 30
Fair use policy 31
Business Continuity & Disaster Recovery 31
Redundancy 31
Business Continuity 31
RTO 31
RPO 32
Disaster Recovery 32
Compliance 32
Security Audits & Reports 32
External audits 32
Penetration test 32
Customers on-demand Audits 33
Internal audits 33
Vulnerability scan 33
Static Code Analyzer 33
Insurances 34
Is Ibexa ISO 27001 or ISO 27701 certified? 34
Data protection and privacy 34
Ibexa as “data processor” 34
PII Retention Policy 35
IP addresses 35
Restitution of Data at the end of the contract 35
Ibexa GDPR protection measures documentation 35
Organisational measures to ensure security and protection of PII 36
Data Protection Officers 36
Human resource measures 36
Confidentiality clause in employment contracts 36
Security awareness and continuous education of staff 36
Data Breaches procedures 37
Incident intake 37
Assessment of the incident 37
Incident handling 37
Handling the “Security” aspect of the incident 37
Handling the “Privacy” aspect of the incident 38
Incident closure 38
Transfer of PII to the customer 39

Automatically push of PII to customer's information system 39
Manual transfer of PII to customer 39
Technical measures to ensure security and protection of PII 39
Privacy by design and by default 39
Cookie Management 40
Deletion of PII 40
Restricted access to production Personal Data 40
Physical access to our offices 40
Computers 40
IT security controls 40
Contractual agreements with Customers 41
Data Processing Agreements 41
Records of Processing activities 41
Ibexa's sub-processors 42
Artificial intelligence and Compliance 43
Annex 1: Definitions 44

Introduction

What is “Ibexa Agentic Marketing Platform” ?

The Ibexa Agentic Marketing Agentic Platform (in short “IAMP”) is a multi-tenant AI operations platform that helps organizations create, run, and govern AI-powered agents. It connects language models with approved external tools and company knowledge so teams can automate repeatable work, support users with an AI assistant, and manage usage in a secure organizational environment.

Why this document?

This document aims to provide an overview on the Information Security Management System (ISMS) in place within Ibexa. It will help prospects, customers and suppliers to assess the maturity of Ibexa’s information security.

Audience of the document?

This document is intended to 3rd party risk assessors, security departments, information security auditors, CISO, or IT departments of prospects, customers and suppliers.

How to use the document?

The document is structured to follow the domains of the ISO27701 framework and provide excerpts from our internal policies that are declassified for use by the intended audience outside our organisation.

The document has to be read with its annexes that contain definitions, as well as references.

Information Security Management System (ISMS)

The CIO and DPO are managing respectively the Information Security and Data Protection at Ibexa by running a state-of-art ISMS (Information Security Management System) and PIMS (Personal Information Management System) , following the ISO27701 international standard.

The ISO27701 standard is used as the framework to manage, with a systematic and exhaustive approach the security of information through its life cycle within Ibexa.

Organisation of information Security

Policies and Procedures

The ISMS and PIMS are composed of a set of Policies, Procedures and Supporting Documents that are created, reviewed and approved by the Management of Ibexa.

The ISMS and the PIMS are communicated to all staff members of Ibexa, and are explicitely part of the contractual agreement of staff members with Ibexa. The contractual agreement is also referring to the disciplinary process in place in case of violation of the ISMS and PIMS.

Moreover, the ISMS and PIMS are part of the awareness program provided to all staff members of Ibexa

Roles and Responsibilities

Information Security is managed at Ibexa by its CIO (Chief Information Officer), directly reporting to the CEO (Chief Executive Officer).

The IT Security unit is composed of **two complementary roles** working closely together:

- a **Technical Security Lead:** Drives the technical implementation of IT and product security, managing security tools, risk analysis, awareness programs, and KPI reporting.

- a **GRC Lead:** Owns security governance and compliance (including ISO27001 roadmap), maintains the internal IT security policies and risk register, and leads third-party interactions such as customer security questionnaires and external auditor coordination.

A DPO (Data Protection Officer) has been appointed by Ibexa to answer questions related to the protection of PII (Personally Identifiable Information).

These responsibilities are spread over multiple persons in order to provide a clear segregation of duty while operating the ISMS and PIMS.

Ibexa policies are approved by Senior Management of Ibexa for their adherence to the company's strategy before being rolled out to the company.

Risk Management

Risk Management Methodology

The risk management methodology run by Ibexa is evaluating risks based on the impact if a risk is getting real, and the likelihood of its realisation. Both, impact and likelihood, are scored on a scale of 1 to 5. The final score of a risk is then evaluated by multiplying its impact by its likelihood.

A risk appetite is defined with Senior Management and risk above the risk appetite are treated.

The possible treatments of a risk are:

- **Mitigation**: Selection of security control or controls from Annex A of the ISO/IEC 27001 standard or some other security controls
- **Transfer**: Transferring the risks to a third party – e.g. by purchasing an insurance policy or signing a contract with suppliers or partners
- **Avoidance**: Avoiding the risk by discontinuing a business activity that causes such risk
- **Acceptance**: Accepting the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialise

The risk register is owned by the GRC Lead and is reviewed yearly. The risk appetite is decreased at each iteration of the risk assessment.

Human Resource Security

Candidate selection and Screening

Ibexa's staff is selected through a screening process where their skills and adherence to the culture of the company are assessed.

Onboarding process

Each member of the staff is following an onboarding process during which they are following training (up to 10 weeks) in order to ensure that the resource has the skills needed to perform the job. The learning curve is assessed weekly with the manager and a "Ibexa buddy" (internal mentor to help the new hire in its learning curve) that is assigned at the hiring of the person.

A final assessment is performed at the end of the onboarding process of the new-hired in order to verify the knowledge of the person on the product and the process within the company.

Security awareness and continuous education

Ibexa has deployed a training and awareness program towards its staff.

Training and awareness sessions are performed

- On person: through ad hoc training for limited audience or during our "General company meetings" performed 2 times a year for global audience
- Online: through an eLearning platform to deploy training campaign along the year

Specific attention is given to data protection and privacy though:

- Recurrent training sessions regarding Security and Privacy provided by the IT security team, DPO or legal team
- Specific GDPR and security workshops for developers & product managers;

Offboarding process

Each leaver of the company will follow a strict offboarding process to ensure, thanks to the asset and user access inventories, that every asset and user access are deprovisioned or returned to the company.

Confidentiality Clause in Employments Contracts

All our employment contracts include mandatory confidentiality clauses in accordance with GDPR.

Asset management

Asset inventory

Ibexa's assets as well as 3rd party assets on which the company depends on are assessed once a year. All assets are logged into an asset inventory with the assignment of an owner and the classification of the asset based on its criticality for the company.

The responsibility for the asset inventory and its annual review is the responsibility of the GRC Lead.

Information Classification

A formal Information Classification has been crystallised into a policy ruling, the classification of information, its owner, its treatment, handling procedures, disposal and destruction.

The current information classifications used by Ibexa are:

- Public
- Business Use Only (default standard)
- Confidential
- Restricted

Access control

Ibexa's Access Control Policy

User administrators have real time access to the list of their users and can upgrade/downgrade rights & access. Details of user rights are available here :

Role	Description
Organisation Owner	The user who owns the organisation. Holds the highest authority within that organisation, including actions reserved exclusively for the owner (e.g. certain organisation-level management operations) in addition to all Organisation Administrator permissions.
Organisation Admin	Manages users, settings, integrations (LLM providers, MCP servers), and resources within their own organisation. Can invite/remove members, assign roles, and configure organisation-level policies.
Organisation Member	Standard end user within an organisation. Can use agents, reports, conversations, and knowledge base features according to organisation settings, but cannot manage users, billing, or organisation configuration.

Administrators retain the ability to disable accounts at any time.

Ibexa's Password Policy

Ibexa's Manager Password Policy

- All passwords are chosen by the user, encrypted in transit and stored as a hash at rest in our systems (see Cryptography).
- Password complexity: password must meet all the following requirements:
  - At least 12 characters long
  - at least 1 number
  - at least 1 capital letter
  - at least 1 small letter
  - at least 1 special character
- Password history:

    - Users cannot reuse their previous 100 passwords (hashed version of all previous passwords are kept in database)
- Password expiration:
    - Password expires after 90 days
- Brute force protection
    - After 10 wrong attempts, a one minute delay is required before the next attempt
    - Each subsequent wrong attempt increase this delay by 1 minute
    - The delay is increased up to a maximum of 15 minutes
    - The number of wrong attempts is reset after 12 hours
- User creation:
    - Invitation is sent by email to the user
    - Link is available for 7 days
    - If the user hasn't logged in after the link has expired, the user must start a reset password procedure
- Reset password:
    - Password reset link is sent via email
    - Temporary: link available for 1 hours
- Temporary password:
    - In case the 'Reset or invitation email' is not received by the user, a temporary password can be generated by the support team and sent to the user
    - The user will need to create a new password on the first login
- Password caching is not allowed
- Session timeout: Back-office sessions last for 45 minutes (which is prolonged by any action performed on the interface eg: click, mouse moved, content edited, etc.)

Single Sign-On (SSO)

Single Sign-On is available with the main identity providers:

- Google (Social SSO)
- Microsoft (Azure Active Directory)

We support as well the following single sign-on protocols:

- OAuth (specifically OAuth 2.0 nowadays)
- OpenID Connect (OIDC)
- Security Assertion Markup Language (SAML)

This solution provides flexibility to our customers to easily comply with their own secure authentication requirements and policies.

MFA (Multi-Factor Authentication)

Ibexa provides a two-factor authentication (2FA) method using a time-based one-time password. This security layer is deactivated by default and can be turned on to re-enforce security.

Admins can enforce the usage of the 2FA.

The time-based one-time password authentication applications supported are FreeOTP and Google Authenticator. The link between the device and the account can be reset by the Admins in the back-office. Once enabled, the 2FA connection is mandatory for every login.

The 2FA can be used with the email-password or the SSO method.

Ibexa strongly recommends their users to use the multi-factor authentication provided through the integration with their Identity Provider (see Single Sign-On).

User Creation

New users receive an email invitation link valid for 72 hours and are required to set a new password on initial login.

New users are provisioned in an inactive state and receive a single-use, time-limited (72-hour) invitation link by email. The system validates the link before presenting the activation form, where the user sets their password and may optionally complete their profile.

Upon successful activation, the account becomes active, the invitation token is consumed, and the user is automatically signed in. Expired, reused, or invalid links are rejected, and administrators can reissue a fresh invitation if needed.

Session Timeout

User sessions automatically time out after 60 minutes of inactivity.

Segregation of duty

Ibexa has implemented internal technical processes to restrict sales staff to access client's data and environments.

Least access privilege

Ibexa staff members are provided with the minimal access required to perform their duty.

Onboarding, offboarding, change of position & periodical reviews

Organisational processes are in place to control the provisioning and deprovisioning in case a staff member is joining, or leaving, or changing his/her position in the organisation.

Accesses are reviewed periodically by asset owners in order to verify the accuracy of accesses to their assets.

Multi-tenant and Segregation of data

1. Authentication and tenant identification

- Users authenticate with signed, time-limited access tokens (JWT).
- The token identifies only the user. The user's organisation is looked up from the database on every request and is never taken from data the client sends. A user therefore cannot act on behalf of another organisation by changing request parameters.
- On every request the platform checks that both the user account and its organisation are active. Blocking or deactivating a user or an organisation takes effect immediately, not when the token expires.

2. Tenant tagging of data

- All customer data is linked to its owning organisation, either directly or through the record it belongs to. This covers agents, conversations, executions, messages, files, knowledge-base documents, integrations, reports, credits and notifications.
- Knowledge-base content used for AI retrieval (document chunks and their vector embeddings) carries its own organisation identifier, which is checked on every search.

3. Scoped data access

- All database queries for customer data are restricted to the requesting user's organisation.
- If a user requests a resource that belongs to another organisation, the platform answers as if it does not exist ("not found"). It does not reveal that the resource exists elsewhere.
- Shared platform resources, such as the public catalogue of agents and integrations or AI model definitions, contain no customer data. Shared AI model providers are made available to an organisation only by explicit assignment from a platform administrator.

4. Authorisation within an organisation

- A dedicated authorisation layer checks every operation against role-based rules: organisation owner, organisation administrator, member, and the creator of the resource.
- For example, only the creator, an owner or an administrator can modify or delete an agent. Conversations are visible only to the user who created them. Members see only the executions they started.
- When resources are linked to each other (for example, a tool or a sub-agent attached to an agent), the platform checks that both belong to the same organisation.

5. Background processing

- Asynchronous jobs, such as agent executions, document processing and evaluations, carry the organisation identifier. Each job reloads its data with the same organisation restriction as interactive requests.
- Real-time streams and temporary caches are reachable only after the request has passed the authorisation checks above. Cache entries that hold organisation-specific results include the organisation in their key.

6. File storage

- Uploaded files and knowledge-base documents are stored under organisation-specific storage paths.
- Files can be downloaded only through the platform. Download links are short-lived and bound to a specific file, conversation and organisation.

7. AI agent access to customer knowledge

- The built-in knowledge-base tool used by AI agents runs with the permissions of the user on whose behalf the agent acts. The AI model is never given organisation or user identifiers.
- An agent can additionally be limited to specific folders of its organisation's knowledge base.

8. Inbound integrations (webhooks)

- Inbound webhook calls are matched to their organisation through a unique, unguessable token
- They can also be protected by an IP allowlist, an HMAC signature with timestamp validation (protection against replay), and rate limiting. Rejected attempts are recorded in an audit log.

9. Verification

An automated test suite runs in the continuous integration pipeline. It includes tests that check that data from one organisation cannot be accessed by another, at the database-access level and at the API level.

Cryptography

The following requirements for cryptography have been defined:

- Production servers
    - In transit : encrypted
        - Encryption algorithm : at minimum AES-256 (cf cipher suite)
        - This encryption algorithm is accepted by NIST Special Publication 800-52
    - At rest :
        - Filesystems: Every server containing personal data have their filesystem encrypted (Bitlocker solution for Windows based servers, AES-XTS for Linux based servers)
- Backup locations
    - In transit : at minimum AES-256 (cf cipher suite)
    - At rest : Filesystems have their filesystem encrypted with AES-XTS
- Sensitive data (API keys, SSO configuration Variable,...): Sensitive data are encrypted with AES-256 with a key provided at runtime to the application.
- Access to production servers: SSH Private key is mandatory in order to get access to production servers. These accesses are limited to a limited subset of Ibexa staff based on a ”need to know” and “least access privilege” principles
- Only trusted and non-compromised certificate authority (CA) are used for production purpose
- The creation, distribution, storage and deletion of certificates is strictly managed by the CTO, or automatically (programmatically) setup under his supervision

Encryption of data at rest

The following table summarises the encryption at rest in our infrastructure and key management:

Name	Company HQ	Datacenter location	Transferred PIIs	Encryption at rest	Encryption key owner
OVH	France	EU	Agent data System & access & applicative logs	Y (HDD level) Y (HDD level)	Ibexa Ibexa
AWS	USA	EU	System & access & applicative logs	Y (applicative)	Ibexa

Encryption of data in transit

From To	OVH	AWS	CDN77
OVH		TLS	TLS
AWS	TLS		TLS
CDN77	TLS	TLS	

Physical and Environmental Security

Thanks to the asset inventory maintained by Ibexa, the location of each mission critical information and IT assets is known. A policy is rolling out in order to ensure that these assets are located in a data processing facility compliant with ISO27001 and/or SOC2 standards.

Data processing facilities

Our core-business applications are located inside datacenters of the OVH group, which are ISO27001 and SOC2 compliant, ensuring the use of:

- Strict visitor policy
- Alarm system
- Video surveillance equipment (CCTV)
- Fire prevention
- Climate control systems
- Redundancy of power and telecommunication supplies
- ...

Our current footprint in terms of geographical spread is 700 km across Europe.

More information about the physical & environmental security can be found under the sub-processors section.

Ibexa's Offices

- Access to our offices is secured.
- Offices are locked outside of office hours.
- No data is hosted in our offices.

Ibexa's laptops

Ibexa laptops are governed by a "Secure EndPoint Device Policy" that enforces technical and operational measures to protect the device and its content. Laptops are verified periodically for their conformity with the policy.

The policy defines, amongst other measures:

Hard drive encryption

In order to prevent data leakage due to theft of a Ibexa's laptop, data encryption of hard drives is enforced. The full list of encrypting keys is kept by Ibexa, the hard drive being crypt-erased (by deleting the encryption key), once an employee leaves the company.

Antimalware protection

Ibexa laptops are protected by an antimalware protection that is always active. This antimalware protection is managed at the company level for all Ibexa laptops.

Software updates

Laptop must always be updated to the latest stable version of the software (application and operating system) provided by the editor.

Clear screen, device locking and unattended devices

If the authorised person is not In direct control of the device, all sensitive information must be removed from the screen.

In the case of short absence, the clear screen policy is implemented by locking out of all systems or locking the screen with a password or biometric security (fingerprint). Auto locking rule must be set to lock Mobile Computing Device automatically after a defined period of time.

In the case of longer absence (eg: holidays), the user must log out from his session.

The policy is also ruling the fact that laptops should never be left unattended if not in a secure area.

In case the device is left at the office outside business hours, it must be placed in a locked cabinet.

USB Mobile Storage Device

It's strictly forbidden to use any USB mobile storage device on any asset of the organisation. Please refer to the data classification policy for the allowed platform to store or share (internally or externally) Ibexa's data.

Operations Security

Backup Policy

The following types of data are part of our Backup policy:

- Databases
- User provided content hosted by Ibexa
- Documentation
- Internal Files

- Emails
- Application code

Backup of databases

Ibexa's databases host the most sensitive and mission critical information of the company.

For this reason, all databases containing PII data are:

- Replicated:
    - Data records are replicated in real time on at least two database nodes, located in distinct datacenters.
    - The replication is ensured via an encrypted channel.
- Backed up:
    - All databases backups are encrypted
    - The storage is performed on any of Ibexa EU datacenter
    - Retention period is 180 days.
- Testing of backups:
    - Backups are tested for integrity. Because we use multiple database technologies according to the type of data that must be stored, the testing of backups is performed on databases using a "round robin" scheduling over the different exercises.
- Frequency of backups:
    - Backups are performed on the multiple database technologies in order to comply with our defined RPO (Recovery Point Objective) and RTO (Recovery Time Objective).

Backup of User Provided Content hosted by Ibexa

Content provided by our customers is stored between multiple Ibexa EU data centers (object based storage). Content is versioned and replicated in order to meet our RTO/RPO.

Documentation & internal files

Documentation and internal files are hosted on Google Drive (Data region enabled is Europe). Backup of this data is ensured by Google, as part of the data region policy (https://support.google.com/a/answer/9223653).

Emails

Our emails are hosted by Google Mail (EU servers), their backup is ensured by Google.

Application code

Application code is versioned through GIT, backup of the git repository is ensured via regular checkout of the repository. A mix of GitHub and internal GitLab instances are used.

DDoS and Firewalls

The complete Ibexa's application infrastructure is protected against DDoS (Distributed Denial-Of-Service) by the OVH Anti DDOS infrastructure. After this line of defence, our infrastructure is protected by network equipment performing load-balancing and traffic throttling / rate limiting, as well as a firewall to deny access to non-public services and protect from common attacks.

Logging & Monitoring

Ibexa has put in place adequate tools to log, monitor and alert teams in real-time in case a suspicious behaviour is detected.

All logs (application and system) are already shipped and aggregated inside an Elasticsearch cluster. The following platform are used to support our logging, monitoring and alerting needs:

- Monit: reactive monitoring + alerting and implementing safeguard or emergency measures to win precious minutes when something happens.
- ELK Stack: Logs aggregation to centralise all events on the platform.
- Uptime & FreshPing : External monitoring of our services
- Prometheus with Alert manager
- External port scanner to detect change of surface attack of the infrastructure

Remote access control & Intrusion Detection & Prevention

All our servers are protected against intrusions by exclusive access through a management VPN, in conjunction with a protection against brute force attacks. SSH access is always based on private-key authentication.

Services exposed to the internet only do so via the HTTP protocol and are protected by a Level 7 Filtering HTTP-proxy.

IDS is implemented through the use of Unix audit events gathered and centralised on a separate server from the one under surveillance.

Communications security

HTTPS and SSL

Traffic between Ibexa server and end-users browser is encrypted using TLS 1.2 & 1.3 only

The cipher suite used is `EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH`

Information Systems Acquisition Development and Maintenance

Secure Development Lifecycle (SDLC)

Scrum methodology and Kanban frameworks are used in order to drive and manage our developments.

Each request is assigned a type being:

- Features: A new feature for the product available to all our customers
- Bug: A correction to an existing feature of the product. Bugs also include incidents.
- Customer project: A specific request for one customer such as custom integration.

Features

All features are defined using “User Stories” created together with the Product owner, a representative of the development and QA teams.

Features are analysed from a security and privacy perspective in order to ensure Privacy and Security by design and by default.

Features are scheduled into Sprints as soon as they reach the “Ready” state.

In order to ensure the quality of developments, Ibexa uses strict definitions to define that a User Story is "Ready" (ready to develop) and “Done”.

Bugs

All bugs are evaluated by the Product team and, based on their criticality, are scheduled in a future Sprint or retrofitted in the current sprint.

Customer projects

All customer projects are handled by Project Managers that make the link between the customer and the internal development process. User stories for customer projects are defined and are scheduled into the future sprints.

Teams

We have multiple teams working together to develop, maintain and evolve the Ibexa software:

- Product team (PT)
- Quality Assurance team (QA)
- Agile Development team (Dev)
- Infrastructure team (IT)

Development practices

Ibexa maintains and operates a single codebase for all its clients. This code is developed with a strong focus on quality and performance. To achieve these goals, different techniques and coding standards are used such as:

- Pair programming
- Test Driven Development
- Code reviews (human and AI based)
- AI generated code

Ibexa tries to avoid big-bang and/or reinventing the wheel. For these reasons Ibexa is:

- Using continuous integration and deployment for small, incremental steps
- Using framework and components whenever it's possible (mainly on new applications)
- Evolving existing applications instead of re-starting from scratch

Separation of environments

Environments are separated and only production servers contain real “personally identifiable information” (PII) and/or actual customer data, developers and testers are working on dummy test data in the respective environment (development, Q&A).

Environments accesses

Ibexa has different environments, for development, QA, acceptance and production. Database access is restricted per user on an **assigned role** basis, and per application on a **scope** basis. Access to the production database is limited to a very limited pool of users.

The IT security team is responsible for assigning a role, per environment, to each member of the IT team.

High level architecture

Multi-tenant SaaS platform (backend API + web frontend) for AI agent orchestration. Tenants are isolated logically as Organisations, with all domain data scoped by an organisation identifier.

Key Components:

- **Frontend** - single-page web application for configure and work with Ibexa Agentic Marketing Platform.
- **Backend API** - stateless, horizontally scalable service; domain-driven design covering users, organisations, agents, conversations, knowledge base, credits, etc.

- **Worker** - asynchronous task-processing service handling background/scheduled jobs (e.g., long-running agent executions, notifications, scheduled triggers) decoupled from the request/response cycle of the API.
- **Relational database** & **Vector Store** - primary datastore for structured data and embeddings .
- **Cache** - in-memory store for caching and scheduling metadata.
- **Message broker/queue** - mediates asynchronous work between the API and the Worker.
- **Object storage service** - stores files, avatars, and images.

Code review & Testing

The technologies we use include the most advanced frameworks & software components: Redis, NodeJS and React.js.

All Ibexa's components have been developed internally and are updated by our IT team.

Peer Code Review

All code ready for production is countersigned by at least 2 internal developers and AI Agent / Github Copilot .

Testing

Testing is a crucial part of our product development, that's why we have a full time team of QA internally. Testing is performed manually and automatically.

Ibexa uses a mix of:

- Unit tests: automated, application-level
- Integration tests
- End-to-end tests
- Manual regression testing
- Pre-production End user simulation

We make use of automated tests whenever it's possible through a test platform (like Postman for all API regression tests).

These tests are automatically triggered by our continuous delivery platform.

Release Management

What is Release Management?

Release management is the process of managing, planning, scheduling and controlling a software build through different stages and environments; including testing and deploying software releases

Release Management ensures that we are delivering new features while protecting the integrity of existing services.

Objectives

- Ensure a high number of successful Releases, i.e reducing the number of Releases with unexpected outcomes or requiring roll-back.
- Maintain a low number of incidents caused by Releases.
- Create a single documented process for managing all Releases.
- Ensure that the process is adopted and escalated to management if there are compliance issues.
- Improve productivity by establishing standard release processes and tooling.
- Harvest lessons learned from the Release Management process that could be applied to other areas of Service Management.

Policies

- All projects, bundled changes to an existing service (releases containing multiple enhancements/fixes) and critical changes to an existing service must go through the Release Management process with appropriate approvals (Head of Product or Product Team / Customer Project Team, DPO and CIO).
- Whenever possible, changes to an existing service should be bundled together and released on a regular (weekly) basis using the Release Management process.
- A single "Release Manager" must be identified for every Release. The Release Manager will be responsible for successful coordination and execution of the Release, as well as ensuring all required documentation related to the Release exists.
- Each Release should be well tested and verified prior to implementation by our QA team.

- All implementation work on the Release should be completed by the Planned End Date/Time.
- Validation that the Release has been completed successfully should be confirmed through post-release testing.
- Introduced changes maintain backward compatibility, and any deprecations or removals are communicated at least 2 weeks in advance. A detailed changelog is available on the Release Notes page: https://docs.ibexa.ai/release-notes

Release Workflow

- All features/tickets are available in pre-production environments.
- All features/tickets are reviewed by QA on pre-production environments.
- All features/tickets are updated with the correct label: Production Ready.
- Release Maintenance is flagged as started on the status page.
- Preproduction environments are merged into production environments.
- Release is correctly tagged.
- Release Note link is added to Git tag
- Release Note is fully completed (correct expected/spend time, presences, all tests green).
- Release Maintenance is closed on the status page.
- Release Communication (internal and external).

Lesson Learned

Each regression identified in the release must have a post analysis on problems we encountered. These information will be attached to the internal Release Note:

- Description
- Severity
- Impacts
- Solutions to observe for next releases
- Details

Production Data

Production data is restricted only to the production environment. Developments and testing are performed on dummy test data.

Information Incident Management

Incident Management Procedure

Ibexa has implemented an Incident Management Procedure. It handles appropriate duties for responding to, mitigating and to remedying Security and Privacy incidents. The policy is available on-request.

Customer Support

Status Page

A status page is available at : https://Ibexa.status.io/ with the possibility to register for notifications via email, webhook, RSS, etc

Online assistance

All Ibexa's users can contact the Helpdesk https://www.support.Ibexa.co and support.agentic@ibexa.ai email address.

Standard Support is available during regular Office Hours (Monday to Friday, 09:00–18:00 UK & France local time), including public holidays.

Service Uptime

Component	Uptime	Description
Agent Runtime	99,0%	The underlying infrastructure layer that executes, manages, and secures AI agents in production.
Agent Administration	95,0%	The back-office environment where agents are built, configured, and managed.

Response times

First response and mitigation times measured within Office Hours:

Priority	Estimated first response time	Mitigation time
P1	2h	8h
P2	4h	72h
P3	8h	1080h
P4	Best Effort	Best Effort

Mitigation times are objectives. Depending on the volume and priority of requests submitted to Support, response and resolution times may vary.

Technical vulnerabilities management and Patching policy

Technical vulnerabilities patching

Technical vulnerabilities patching is prioritised based on the "Common Vulnerability Scoring System"(CVSS) as follows:

	Critical	High	Medium	Low
Patching delay as from notification	48 hours	48 hours	15 business days	60 business days

Other patches and updates

Patches are handled during the regular maintenance week included in the team's roadmap. At least two maintenance weeks must be scheduled for each quarter.

How: maintenance task in the next maintenance week

Major version changes

Major version changes for project dependencies and infrastructure components have to be planned and handled through a project included in the team's roadmap.

Time frame: 6 months

How: detailed project included in the roadmap

Fair use policy

- The Ibexa systems work as a distributed application, the system uses a load balancer to steer users to a computing node
- The basic resources are shared across all customers, requests will be sent to the least active server based on recent activity history
- Ibexa may take reasonable measures to safeguard the stability of the system. These measures and the conditions are described in our terms of use.

Business Continuity & Disaster Recovery

Redundancy

In order to ensure its high SLAs, Ibexa makes use of 3 data centers: Frankfurt (DE), Gravelines (FR) and Roubaix (FR) , all ISO27001 and SOC2 Type II certified.

This setup ensures a geographical spread of 700 km across Europe.

Business Continuity

Ibexa has defined business continuity scenarios that respond to disruptions due to Environmental, Technical or People factors.

Those scenarios have been defined to meet the RTO and RPO approved by the Management.

RTO

RTO (Recovery Time Objective) is the maximum time during which data is unavailable.

All backup solutions deployed in Ibexa should ensure a RTO of maximum 24h, when they protect Ibexa's customer data. When the protected data is Ibexa's internal data, this RTO should not exceed 48h.

RPO

RPO (Recovery Point Objective) is the maximum time since the last backup point. It quantifies the maximum amount of data that can be lost.

The RPO is of maximum 24h.

All the metrics above should apply 99% of time. Due to the way backup and replication works, it is acceptable to have punctual exceptions to these timing.

Disaster Recovery

A disaster recovery procedure has been defined by the CTO to recover the production systems in case of disaster (recovering from scratch). The disaster recovery applies for all production systems needed to provide the Ibexa service to our customers. This disaster recovery procedure is reviewed yearly.

Compliance

Security Audits & Reports

Ibexa is running periodic assessments on the security of the product. They can be performed by a 3rd party (external audit) or internally (internal audit).

External audits

Penetration test

A penetration test is an authorised simulated cyberattack on Ibexa's infrastructure and application, performed to evaluate the security of its platform. The test aims to identify vulnerabilities, including the potential for unauthorised parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

Ibexa is contracting with external parties to conduct penetration tests missions 2 times a year.

A declassified version of the pen test report is available upon request for our active customers by contacting security@Ibexa.co.

Customers on-demand Audits

Ibexa works with more than 1200 enterprise organisations across Europe in various sectors (media, banking, retail, FMCG, etc.). Each of our clients has high security and data protection standards. This is why Ibexa is willing to share the results of audits (with them in order to guarantee the existence, monitoring and continuous improvement of its management systems related to the Information Security (ISMS) and PII (PIMS); by external auditors.

This mechanism has been put in place in order to prove our compliance with international standards and facilitate security assessments from customers, which is time-consuming on both sides.

Similar to most Saas companies in our yearly licence price range, we do not allow our customers to organise their own audits of Ibexa, as those exercises are highly time-consuming for our teams. As a fast-growing company it does not scale to follow up different custom audits.

Additional on-demand security audits requests (security assessment and penetration tests) or requirements can be analysed by our GRC Lead for Platinum customers only. Please refer to our General Terms & Conditions & take contact with your account manager if you have any questions related to on-demand audits.

Internal audits

At the same time, Ibexa is running audits internally. These audits include:

Vulnerability scan

Ibexa is constantly scanning its infrastructure against open ports or well known vulnerabilities.

Docker images are signed and scanned for vulnerabilities before being deployed.

Static Code Analyzer

- Sonarqube and Github Copilot are used as Static code analyser

Additionally language specific tool: Ruff, Mypy, Biome, TypeScript compiler

Insurances

Ibexa's activities are covered by the following insurances:

- Professional Indemnity Cover and Public Liability Cover
- Cybersecurity cover

Is Ibexa ISO 27001 or ISO 27701 certified?

No, Ibexa doesn't hold an ISO certification for the moment.

We've implemented an Information Security Management System (ISMS) and a Private Information Management System (PIMS) respectively based on ISO27001 and ISO27701 standards.

Those Management Systems are regularly reviewed and improved. This document, based on the structure of the ISO controls is a proof of our commitment and adherence to those ISO Standards.

We also make sure that our suppliers are as secure as us. Indeed, our supplier security policy requires that all our sub-processors, that are processing customer's information, must be ISO27001 certified or provide a SOC2 Type 2 report.

Convinced by the importance of an ISMS and PIMS, the Management is fully supporting the Management Systems and their continuous improvement. However, it is a Management decision to not enter in the ISO27001 certification process, based on the current size of the company and its agility (time to market).

Data protection and privacy

Ibexa as “data processor”

The IAMP can, by its generic nature, process a lot of different data types. The type of data that will be processed by the system is dependent on the decision of the customer.

When personal data are processed by the platform, Ibexa acts as a « data processor », processing data on behalf of its clients (the « data controller »).

Accordingly, Ibexa has no direct relationship with the individuals whose information it receives from its clients. Ibexa does not control such information, does not select or determine the specific types of data it processes, and does not determine the purpose for which it is processed.

PII Retention Policy

IP addresses

IP addresses are PII for which specific processing is performed by our systems.

Within the underlying technical infrastructure, Ibexa may keep the IP addresses of the visitors, for a period not exceeding six (6) months, in order to have the necessary traceability to ensure the security of its information system and its products and services. These access logs allow Ibexa to analyse accesses to its systems and platforms and determine the origin of possible incidents and alerts (fraudulent access, misuse, etc.) by establishing correlations between log data. These access logs are not used for any other purpose than technical and organisational security.

This is a recommended retention period from a security perspective (to have historical data to investigate in case of an incident), and an acceptable delay acknowledged by data protection authorities.

Restitution of Data at the end of the contract

Clients can request the export and delete Data at all times. Customer databases and accounts are permanently deleted within 1 month after contract termination.

Ibexa GDPR protection measures documentation

This is where you'll find Ibexa's standard GDPR agreement, along with our other measures for data protection. Those documents will be updated in time to reflect our latest measures.

Organisational measures to ensure security and protection of PII

Data Protection Officers

In order to ensure the independence of the Data Protection Officer, we've appointed a DPO who is reachable through the email dpo@Ibexa.co.

We ensure that our Data Protection Officer

- Is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data.
- do not receive any instructions regarding the exercise of those tasks.
- are bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.
- won't be dismissed or penalised by the Controller or the Processor for performing his tasks.
- don't perform any such tasks and duties do not result in a conflict of interests.

Ibexa will support the Data Protection Officers in performing the tasks referred to in Article 39 of the GDPR by providing the resources necessary to carry out those tasks and access to Personal Data and processing operations, and to maintain his or her expert knowledge.

Human resource measures

Confidentiality clause in employment contracts

See "Confidentiality Clause in Employments Contracts" section

Security awareness and continuous education of staff

See 'Security awareness and continuous education' section

Data Breaches procedures

Incident intake

Anyone can notify Ibexa of a security and/or data breach through the following email addresses: dpo@Ibexa.co and/or security@Ibexa.co.

The following information must be provided:

- the nature of the data breach
- categories of data impacted
- number of records
- number of data subjects
- any other information that led you to presume the data breach
- contact details (DPO or any other contact point)

If the information is not sufficient, the person that is investigating the incident will request more information from the person that has reported the breach to Ibexa.

The DPO team and/or the Security team will acknowledge your request then immediately start to investigate your potential data breach case. An incident ticket will be created in the ticketing system of Ibexa.

Assessment of the incident

The DPO and/or Security team will assess the incoming incident. This investigation will classify the incident in the following cases:

- False positive
- Security breach without PII breach
- Security breach with a PII breach

In case of a “false positive”, the incident will be updated in the ticket management system of Ibexa and the incident will be closed.

Incident handling

Handling the “Security” aspect of the incident

The security team will go through the following activities:

- Containment: The impacted systems will need to be isolated from the operational environment in order to avoid the incident to spread to other assets
- Mitigation (optional): The security team will provide a temporary solution in order to fix the issue until a remediation is available
- Remediation: The security team will provide a permanent solution to fix the issue

Handling the “Privacy” aspect of the incident

The DPO team will perform the following activities:

- Assess the breach: The DPO team, with the needed resources will need to assess the breach. This assessment will need to conclude on:
    - The category of data that has been breached
    - The quantity of data that have been breached
    - The impact on the data subject due to the breach
- Notification: As a data processor, Ibexa will inform the data controller without undue delay with the following information:
    - the nature of the data breach
    - categories of data impacted
    - number of records
    - number of data subjects
    - contact details (DPO or contact point) where more information can be obtained
    - Measures taken or proposed to be taken to address the personal data breach (including when appropriate, measures to mitigate possible adverse effects)
- Document: Ibexa will also document the data breach detected in a record of personal data breaches.

At any stage of an incident, and whatever its category (security and/or privacy), Ibexa could request the intervention of a digital forensics in order to collect legal evidence of the breach.

Incident closure

After that the incident has been handled, a “post mortem” analysis will be performed and documented. This report will contain:

- The root cause analysis
- A timeline of the incident
- Lessons learned
- Action plan

The CISO will make sure that the incident has been correctly documented in the ticketing system. In case of a PII data breach, the DPO will make sure that the incident has been correctly documented in the personal data breach register.

Transfer of PII to the customer

Automatically push of PII to customer's information system

Ibexa is able to push data collected in different ways:

- Real Time Push (REST over HTTPS)
- FTPS Push/Export
- Amazon S3 Bucket Export

Please find more information in this FAQ :
https://Ibexa.zendesk.com/hc/en-us/articles/360019072914-Push-export-data-to-your-CRM-Marketing-Automation-Platforms-other-MarTech-softwares

Manual transfer of PII to customer

Transfer of data exports outside Ibexa is only allowed through a strict procedure to ensure that the correct file has been received by the correct recipient. Based on the data classification of the content of the file, one or more of the controls will be activated:

- Send a temporary link to the file to the recipient email address
- Limit the number of download of the file
- Encryption of the file and send the encryption key through a second secure channel

All accesses (export and consultation) of customer data by the Ibexa staff are logged in the GDPR Toolbox.

Technical measures to ensure security and protection of PII

Privacy by design and by default

We are also implementing a policy of 'Data Protection by Design and Default' to ensure we are systematically considering the potential impact that every project or initiative might have on the privacy of individuals. This is especially sensitive with the Product people at Ibexa (designing new features) and, of course, the IT team.

Cookie Management

Cookies and their usage are described in our "Cookie Policy", which is available upon request to dpo@Ibexa.co.

Deletion of PII

When a deletion request is triggered from the GDPR Toolbox, the related PII are anonymized in order to keep them in an aggregated form in the statistical module.

This anonymization of PII is propagated to all database instances. The PII residing into our archives will be destroyed after the retention period of the backup.

All hardware containing PII that needs to be decommissioned will follow a secure deletion procedure of all its hard drives (using hdparm secure deletion tool) before being removed from our infrastructure.

Restricted access to production Personal Data

See "Production Data" section

Physical access to our offices

See "Physical and Environmental Security" section

Computers

See Ibexa's laptop section

IT security controls

Please refer to sections:

- Asset management
- Access control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications security
- Information Systems Acquisition Development and Maintenance
- Information Incident Management
- Business Continuity & Disaster Recovery
- Compliance

Contractual agreements with Customers

As part of our contractual agreements with customers, the following GDPR related documents will be issued:

Data Processing Agreements

Clear contractual agreements with clients according with article 28, namely impeding Ibexa to disclose, exploit or resell any personal data to third parties ;

Records of Processing activities

In accordance with article 30 (2) of the Regulation, our record of Processing activities includes:

- Our contact details, together with those of the Data Controller on whose behalf you are acting and, where applicable, of the Processor's representative and the Data Protection Officer.

- The categories of processing carried out on behalf of the Data Controllers.
- Where applicable, any transfers of the Data to a third-party country together with documentation showing the existence of appropriate guarantees for each transfer.
- A general description of Technical and Organisational security Measures.

Ibexa's sub-processors

Clear contractual agreements with sub-processors, according with article 28, namely ensure that our Processors provide sufficient guarantees to implement appropriate Technical and Organisational Measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.

Ibexa takes adequate safeguards when transferring personal data out of the European Economic Area (EEA) or outside any country for which an adequacy decision has been made. Standard Contractual Clauses from the European Commission (or other guarantees provided for in art 46 of the GDPR) are contractualized. Next to this, Ibexa assesses (Transfer Impact Assessment TIA) if there is anything in the law or practice of the destination country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools and identifies and adopts supplementary measures when needed (encryption with key management by Ibexa, pseudonymisation, split processing, ...).

Where that other Processor fails to fulfil its Data protection obligations, we shall remain fully liable for the performance of that other Processor's obligations.

Ibexa works with sub-processors to carry out processing activities necessary for the provision of services to the Customer. A list of those sub-processors and related processing activities is located on the Ibexa sub-processors page available from the GDPR Toolbox or at this URL: https://gdpr.Ibexaapp.com/subprocessors.

Artificial intelligence and Compliance

The platform agentic behaviour imply the use of large language model (LLM) based artificial intelligence. AI feature can be provided, by customer decision via:

- Ibexa provided access to multiple LLM vendors
    - These Ibexa model can be provided either by sub-processor of Ibexa
    - Or by LLM models operated on Ibexa server and infrastructure
- Customer provided API keys and model access

The LLM models provider is visible in the application at all times. Customers may restrict access to some provider and/or model.

Key Features of Ibexa's AI Integration

1. Data minimization:
    - The data sent to the AI model is driven by the customer instructions and agent definition. Ibexa will ensure that the smallest set of data relevant for performing the agent activity will be sent to the sub-processor.
2. No Data Used for Training:
    - The API key and account configuration are setup so that data shared with the LLM sub-processor is not utilized for training or fine-tuning the AI models, guaranteeing that user inputs remain confidential and are not stored for model improvement.

Annex 1: Definitions

- “Data Breach” means a Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal data transmitted, stored or otherwise processed;
- “Data Controller” means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- “Data Processor” means a natural or legal person, which processes Personal data on behalf of the Controller;
- “Data Protection Officer” (“DPO”) means a person who is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements;
- “Data Subject” means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- “Organisational Measures” mean the measures relate to the system's environment and particularly to the people using it.
- “Personal Data” means any information relating to an identified or identifiable natural person (‘Data Subject’);
- “Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- “Supervisory Authority” means an independent public authority which is established by a Member State pursuant to Article 51;
- “Technical Measures” mean the measures that directly involve the IT system.