CYBERSECURITY POLICY

AI Usage Policy

Responsible, secure, and approved use of artificial intelligence systems

PREPARED FOR

MIS Solutions, Inc.

Applies to employees, contractors, temporary staff, vendors, and authorized third parties

Policy Field	Value
Version	1.0
Effective Date	[Insert effective date]
Policy Owner	[AI Policy Owner / IT Security / Compliance]
Executive Sponsor	[Executive sponsor name / title]
Approved By	[Approver name / title]
Review Cycle	At least annually and whenever material AI, legal, security or client requirements change
Classification	Confidential - Internal Use Only

Template note: *Replace bracketed fields before adoption and review the final policy with legal counsel and security leadership before issuing to employees.*

MIS

Document Control

Item	Details
Document Name	AI Usage Policy
Business Owner	[Executive sponsor / business owner]
Technical Owner	[IT / Security lead]
Compliance Owner	[Compliance / Legal / Privacy lead]
Related Policies	Acceptable Use Policy; Information Security Policy; Data Classification Policy; BYOD Policy; Incident Response Plan; Vendor Management Policy; Change Management Policy; Records Retention Policy
Policy Review Trigger	Annual review; new AI platform; material vendor change; material security incident; new client, legal or regulatory requirement

Revision History

Version	Date	Author / Owner	Summary of Change
1.0	[Insert date]	[Insert name]	Initial policy release

Contents

1. Purpose and Policy Statement

POLICY BOTTOM LINE

AI may be used for business purposes only when it is approved, secure, appropriate for the data involved, and subject to human oversight. Employees remain responsible for all work they produce with AI assistance.

This AI Usage Policy establishes requirements for the responsible, secure, and compliant use of artificial intelligence systems by MIS Solutions, Inc. It is intended to enable productivity and innovation while protecting company data, client data, regulated information, intellectual property, systems, reputation, and contractual obligations.

This policy applies whether AI is accessed through a browser, mobile app, API, plug-in, integrated software feature, enterprise platform, local model, agentic workflow, automation, security product, or any other AI-enabled service.

Failure to follow this policy may expose the company and its clients to data leakage, inaccurate output, security incidents, intellectual property disputes, regulatory issues, contract violations, and reputational harm.

Policy Objectives

- Enable approved and productive use of AI tools across the business.
- Prevent disclosure of confidential, client, personal, regulated, or security-sensitive data.
- Define which AI systems are covered and how they are approved.
- Clarify employee rights and obligations when using AI on personal devices.
- Require human review, validation, and accountability for AI-assisted work.
- Provide a clear path for questions, support requests, suspected misuse, and incidents.
- Support compliance with applicable laws, contracts, security standards, and client requirements.

2. Scope: Users, Systems, Devices, and Data

Covered Users

- Employees, officers, directors, owners, and temporary staff.
- Contractors, consultants, interns, and outsourced personnel.

- Vendors, subcontractors, and third parties with access to company or client data or systems.
- Any person using company accounts, networks, tools, devices, data, or client environments.

Covered AI Systems

This policy covers all AI systems used for company business, including tools that appear as embedded features inside other applications. Examples are not automatically approved unless listed in the Approved AI Systems Register.

Covered System Type	Examples / Description	Policy Impact
Public or consumer AI tools	Free or public chatbots, writing assistants, image generators, mobile AI apps, and web-based AI services.	Business use is prohibited unless explicitly approved. Sensitive data must never be entered.
Enterprise AI platforms	Company-approved AI tools with business contracts, SSO, logging, retention controls, and administrative oversight.	Use is allowed only within the approved scope and data permissions.
Embedded AI in SaaS applications	AI features in productivity suites, CRM, PSA, RMM, EDR, SIEM, documentation, ticketing, finance, or project tools.	Covered even when AI is only one feature inside a larger approved tool.
AI code assistants	Code completion, script generation, test generation, debugging, and documentation tools.	Generated code must be reviewed, tested, and approved before use.
AI security and operations tools	AI-enabled threat detection, log analysis, endpoint response, vulnerability prioritization, and support automation.	Use must remain defensive, authorized, logged, and consistent with client agreements.
AI meeting and transcription tools	Meeting summaries, call transcription, voice assistants, note takers, and sentiment analysis.	Requires consent where applicable and must follow retention and confidentiality rules.
Generative media tools	Image, audio, video, voice, avatar, and synthetic content generation.	Must not mislead, impersonate, or violate intellectual property, privacy, or client rules.

Covered System Type	Examples / Description	Policy Impact
Agentic AI and automations	AI systems that can take action, call APIs, send messages, change records, create tickets, deploy scripts, or modify systems.	Requires specific risk review, least privilege, logging, and human approval gates.
Local or open-source AI models	Models run on local devices, servers, cloud instances, or client environments.	Requires approval before deployment, training, fine-tuning, or processing company/client data.
AI APIs and integrations	Custom applications, workflow automations, bots, plug-ins, and API-connected services.	Requires security review, vendor review, data flow review, and change management.

Covered Devices and Environments

- Company-owned laptops, desktops, mobile devices, servers, and cloud resources.
- Personally owned devices used to access company systems, company data, client data, or approved AI tools.
- Company networks, client networks, home networks, and remote work environments.
- Production, development, lab, demo, sandbox, and client environments.

Covered Data

- Company data, client data, personal data, regulated data, intellectual property, and confidential business information.
- Prompts, files, images, audio, video, logs, source code, tickets, emails, chat messages, and meeting transcripts.
- Generated outputs when used for company work, client work, records, decisions, automation, or communications.

3. Definitions

Term	Definition
AI / Artificial Intelligence	Software or services that generate, classify, predict, summarize, recommend, automate, reason, search, analyze, or create content using machine learning, large language models, or related methods.
Generative AI	AI that creates text, images, audio, video, code, summaries, reports, designs, or other content.
Prompt	Text, data, files, images, audio, instructions, or context entered into an AI system.
AI Output	Any response, recommendation, content, code, analysis, summary, action, or decision produced by an AI system.
Approved AI System	An AI system that has been reviewed and authorized by MIS Solutions, Inc. for defined business uses.
Shadow AI	Any AI tool, plug-in, account, model, or automation used for business without company approval.
Client Data	Any information belonging to, describing, identifying, or relating to a client, client system, client customer, client employee, or client environment.
Regulated Data	Data subject to specific legal, contractual, or compliance requirements, such as personal information, health data, payment card data, financial data, government data, export-controlled data, or industry-specific protected data.
Agentic AI	AI that can independently plan, call tools, take actions, execute workflows, modify records, send communications, or make changes in systems.
Human in the Loop	A qualified person reviews, validates, and approves AI output or AI-recommended actions before they are relied on or executed.

MIS

4. Governance, Roles and Responsibilities

AI governance is a shared responsibility. Business owners approve use cases. IT and Security approve technical access and safeguards. Employees are accountable for what they enter into AI systems and how they use AI outputs.

Role	Responsibilities
Executive Sponsor	Approves policy direction, risk tolerance, and material AI initiatives. Supports enforcement and resourcing.
AI Policy Owner	Maintains this policy, coordinates reviews, manages exceptions, and supports AI governance decisions.
IT / Security Team	Reviews AI tools, configures access controls, monitors approved systems, supports incidents, and enforces technical safeguards.
Legal / Compliance / Privacy	Reviews data protection, contractual, regulatory, privacy, and intellectual property risks. Advises on disclosures and records.
Business Unit Leaders / Managers	Approve role-based use cases, ensure employee training, and verify AI outputs used in their functions.
Data Owners	Approve whether specific data types may be used with approved AI tools and define handling requirements.
Employees and Authorized Users	Use only approved AI systems; protect data; validate outputs; report issues; follow this policy and related policies.
Vendors / Contractors	Follow this policy, contractual requirements, and client restrictions when using AI for company or client work.

MIS

5. Who to Contact for Questions, Problems or Incidents

WHEN IN DOUBT, CALL BEFORE YOU PASTE

If you are unsure whether data can be used in an AI system, do not enter the data. Contact the IT Service Desk, Security Team, or AI Policy Owner first.

Situation	Primary Contact	Escalation / Notes
General question about AI use	AI Policy Owner: [Name / Email / Phone]	Ask before using a new tool, feature, plug-in, prompt workflow, or AI automation.
Need access to an approved AI tool	IT Service Desk: [Ticket portal / Email / Phone]	Access must be role-based and approved by your manager or system owner.
AI tool is not working or access is blocked	IT Service Desk: [Ticket portal / Email / Phone]	Do not bypass controls or use a personal AI account to work around an outage.
Possible sensitive data entered into AI	Security Incident Hotline: [Phone / Email / After-hours process]	Report immediately. Preserve evidence and do not delete prompts, logs, or chat history unless instructed.
Possible client impact	Security Team and Client Account Owner: [Contacts]	Escalate immediately if client data, client systems, or client deliverables are affected.
Privacy, legal, contractual, or regulatory question	Legal / Compliance / Privacy: [Contact]	Required for regulated data, contract restrictions, disclosure language and external communications.

Situation	Primary Contact	Escalation / Notes
HR or employee conduct concern	Human Resources: [Contact]	Use for policy violations, harassment, discrimination, impersonation, or misuse concerns.
After-hours urgent issue	On-call Security / IT escalation: [Phone / procedure]	Use for suspected data exposure, credential disclosure, system modification, or client-impacting event.

Immediate Escalation Required

- Credentials, API keys, tokens, private keys, client secrets, or passwords were entered into any AI system.
- Client data, regulated data, or confidential company data was entered into an unapproved AI system.
- An AI system sent, posted, changed, deleted, deployed, or approved something without required human authorization.
- AI output caused or may cause a client-impacting error, security issue, contract issue, or public misstatement.
- An AI tool or browser extension requests unusual permissions, access to email/files, or the ability to act on your behalf.

6. Approved AI Systems and Tool Inventory

Only approved AI systems may be used for company business. A tool is not approved simply because it is popular, free, embedded in software, installed on a personal device, available through a client, or used by another department.

Approval Requirements

- A business owner must document the intended use case, users, data types, and expected benefit.
- IT and Security must review access control, authentication, logging, data retention, encryption, administrative controls, and integration risks.

- Legal, Compliance, or Privacy must review regulated data, contractual obligations, vendor terms, intellectual property, and disclosure requirements where applicable.
- The tool must be entered into the Approved AI Systems Register before production use.
- Material changes to features, data usage, model training, retention, integrations or vendor terms require re-review.

Minimum Approval Criteria

Control Area	Minimum Expectation
Identity and access	SSO/MFA where practical, role-based access, least privilege, and timely access removal.
Data handling	Clear rules for what data may be entered, retained, trained on, shared, or exported.
Training and retention controls	Vendor terms must state whether prompts, files, and outputs are used for model training and how long they are retained.
Logging and auditability	Administrative audit logs should be available for business-critical or sensitive use cases.
Security review	Vendor security posture, encryption, vulnerability management, incident notification, and subcontractors must be reviewed for material tools.
Compliance review	Regulatory, privacy, records retention, client contract, and data residency obligations must be considered.
Change control	Agentic workflows, API integrations and tools that modify systems require change management and rollback planning.
User training	Users must understand permitted data, prohibited uses, output validation and escalation expectations.

Unapproved Tools

- Do not use personal AI accounts for company or client data unless explicitly approved.

- Do not install AI browser extensions, plug-ins, mobile apps, or desktop agents that access company systems without approval.
- Do not connect AI tools to email, file storage, PSA, RMM, ticketing, CRM, finance, code repositories, or cloud environments without approval.
- Do not use client-provided AI tools for work involving other clients or company confidential data unless approved.

7. Data Protection and Classification Requirements

DATA RULE

The more sensitive the data, the stricter the AI controls. When the classification is unclear, treat the data as confidential until a data owner, Security or Compliance confirms otherwise.

Data Classification	Examples	AI Use Rule
Public	Published marketing material, public website content, public documentation, public knowledge articles.	May be used with approved AI tools. Verify accuracy before external use.
Internal	Internal process notes, non-sensitive templates, general training material, non-confidential business content.	May be used with approved AI tools if not restricted by business owner.
Confidential Company Data	Non-public financials, strategy, pricing, internal emails, employee records, security architecture, internal reports.	Only use in approved enterprise AI systems authorized for confidential data. Do not use public AI tools.
Client Confidential Data	Tickets, client network diagrams, asset inventories, configurations, project plans, service reports, contracts.	Only use when approved for that client, tool and purpose. Follow client contract and data handling restrictions.

Data Classification	Examples	AI Use Rule
Regulated Data	PII, PHI, payment card data, financial data, government data, export-controlled data or data subject to specific legal obligations.	Do not use unless explicitly approved by Security, Legal/Compliance and the data owner with documented safeguards.
Security Sensitive Data	Passwords, MFA codes, API keys, tokens, private keys, secrets, exploit details, incident logs, EDR/SIEM data, vulnerability details.	Credentials and secrets are never allowed. Other security data requires approved security tools and authorized defensive purpose.
Source Code / Scripts	Application code, infrastructure-as-code, scripts, automation workflows, proprietary algorithms.	Use only approved AI code tools. Do not include secrets. Review licensing, security, functionality and client ownership requirements.

Data Handling Rules

- Never enter passwords, API keys, tokens, private keys, seed phrases, MFA codes, or other secrets into AI systems.
- Minimize data entered into AI systems. Use only what is necessary for the approved business purpose.
- Remove or mask names, account numbers, IP addresses, device identifiers, customer identifiers, and other sensitive details where practical.
- Do not upload full client files, logs, contracts, diagrams, or datasets unless the tool and use case are approved for that data.
- Do not use AI to recreate, infer, profile, or expose personal information without approval.
- Do not override client restrictions. Client data handling rules take precedence when they are stricter than this policy.
- Do not use AI-generated output as a system of record. Save final approved work in the appropriate company system.

MIS

8. Acceptable AI Use

The following uses are generally acceptable when performed with approved AI systems, appropriate data, human review, and business authorization.

Business Area	Acceptable Examples	Required Safeguards
Productivity and writing	Drafting emails, summarizing public content, outlining training, improving grammar, creating templates.	Review for accuracy, confidentiality, tone, and approvals before sending or publishing.
Service desk and operations	Summarizing tickets, drafting troubleshooting steps, improving knowledge articles, triaging non-sensitive issues.	Do not include client-sensitive data unless tool and client use are approved. Validate technical steps.
Sales and marketing	Drafting proposals, campaign ideas, first drafts of collateral, and competitive research using public sources.	Verify claims, pricing, client references, citations, and disclosure requirements.
Software development	Code suggestions, test cases, documentation, refactoring ideas, script examples, and debugging support.	Perform secure code review, testing, licensing review, and change approval before use.
Security operations	Summarizing alerts, correlating indicators, drafting incident notes, improving detection logic in approved tools.	Use only for authorized defensive work. Follow client agreements and incident procedures.
Training and internal knowledge	Creating learning material, role play scenarios, quizzes, and process summaries.	Avoid confidential examples unless approved. Review for accuracy and bias.
Analysis and reporting	Drafting report narratives, summarizing approved datasets, creating executive summaries.	Validate calculations, assumptions, sources, and data permissions.

9. Restricted and Prohibited AI Use

Prohibited Uses

- Entering confidential, client, regulated, or security-sensitive data into unapproved AI systems.
- Entering credentials, secrets, tokens, private keys, MFA codes, or password reset links into any AI system.
- Using AI to bypass security controls, licensing controls, monitoring, DLP, access restrictions, or approval workflows.
- Using AI to impersonate employees, executives, clients, vendors, or public persons without explicit authorization and clear disclosure.
- Using AI to create deceptive content, fake reviews, misleading claims, fraudulent communications, or undisclosed synthetic media.
- Using AI to make final employment, disciplinary, compensation, credit, insurance, legal, medical, or other high-impact decisions without required human and legal review.
- Using AI for offensive cyber activity, unauthorized scanning, exploit development, phishing, credential theft, evasion, persistence, or social engineering.
- Using AI-generated code, scripts, or commands in production or client systems without review, testing, and change approval.
- Uploading copyrighted, proprietary, or client-owned materials in a way that violates license, contract, or confidentiality obligations.
- Relying on AI-generated citations, facts, security advice, legal advice, or technical instructions without verification.

Restricted Uses Requiring Written Approval

Restricted Use Case	Approval Required From
Use of AI with client confidential data	Client account owner, Security and data owner; client approval where required by contract.
Use of AI with regulated data	Legal/Compliance, Privacy, Security, and data owner.
Agentic AI that can modify records, send messages, execute scripts, create tickets, deploy changes, or call APIs	Business owner, IT/Security, Change Advisory authority, and system owner.

Restricted Use Case	Approval Required From
AI tools connected to email, file storage, CRM, PSA, RMM, EDR, SIEM, finance, or code repositories	System owner, IT/Security, and Legal/Compliance, where applicable.
AI used for hiring, HR, performance, compensation, or employee monitoring	HR, Legal/Compliance, and Executive Sponsor.
AI-generated external marketing claims, public statements, or client-facing commitments	Marketing/Sales owner, Legal/Compliance, and Executive Sponsor where material.
Training, fine-tuning, or building models using company or client data	Executive Sponsor, Security, Legal/Compliance, data owner, and client approval where applicable.

10. Human Review, Quality Control, and Accountability

AI output must be treated as unverified draft content until reviewed by a qualified person. The person using AI remains responsible for the final work product, decisions, actions, and communications.

Required Review Before Use

- Confirm the output is accurate, complete, and appropriate for the intended audience.
- Check for fabricated facts, fabricated citations, outdated information, unsupported claims, and missing context.
- Verify calculations, technical procedures, scripts, commands, security guidance, and configuration recommendations.
- Review for confidentiality, privacy, client restrictions, and data classification issues.
- Review for bias, discriminatory language, inappropriate tone, or content that may violate company values or laws.
- Confirm that the output does not include hidden instructions, unsafe code, malicious links, unauthorized data, or leaked prompt content.
- Document review and approval when AI output supports client deliverables, compliance records, security operations, production changes, or high-impact decisions.

External Disclosure

- Disclose AI assistance when required by law, contract, client policy, professional standards or company direction.
- Do not claim AI-generated analysis, testing, legal review, security review or professional judgment was performed by a qualified human when it was not.
- Do not present AI output as final expert advice without appropriate professional review.

11. Client Data, Customer Environments, and MSP Obligations

Because MIS Solutions, Inc. operates as a managed service provider and handles sensitive client environments, client data, and client systems require additional controls.

Client Data Requirements

- Follow the client contract, statement of work, data processing terms, security addenda, and any client-specific AI restrictions.
- Do not use one client's data to support another client, train a model for another client, or create shared outputs that expose client-specific information.
- Do not paste client network diagrams, inventories, tickets, logs, contracts, security findings, or user data into AI tools unless specifically approved for that client and use case.
- Use client anonymization, masking, or synthetic examples where practical.
- Client-facing deliverables assisted by AI must be reviewed by a qualified employee before delivery.
- If a client asks whether AI was used, answer accurately and escalate to the account owner or Legal/Compliance if disclosure language is needed.

Client System Actions

- AI must not independently make changes in client systems without documented authorization and human approval.
- AI-assisted scripts, commands, remediation steps, or configuration changes must follow change management and client approval requirements.
- AI may support analysis, drafting, and recommendations, but employees must validate before client-impacting action.
- Emergency security response remains governed by the Incident Response Plan and client authorization terms.

MIS

12. Personal Device and BYOD Requirements

PERSONAL DEVICE BOTTOM LINE

Using a personal device for company work is optional unless otherwise stated by role. If you choose or are authorized to use a personal device for business, company data and company accounts on that device remain subject to this policy.

Employee Rights on Personal Devices

Right	What It Means
Ownership of personal device	You retain ownership of your personal device and personal content. The company does not take ownership because the device is used for business.
Notice of required controls	You will be informed of required security controls before being granted access, such as MFA, device encryption, screen lock, updates, MDM, EDR, or managed app controls.
Choice to decline BYOD	Where feasible, you may decline personal device use and request an approved company device or alternative access method.
Separation of personal content	The company will focus monitoring and control on company accounts, managed apps, company data and security-relevant access logs, subject to law and investigation needs.
Removal of business access	You may request removal of company-managed apps, accounts or access when you no longer use the device for business, subject to records and investigation requirements.

MIS

Employee Obligations on Personal Devices

Obligation	Requirement
Use approved accounts only	Access company AI tools using company-approved accounts, SSO, and authentication methods. Do not use personal AI accounts for company data.
Meet minimum security controls	Maintain passcode or biometric lock, device encryption, current operating system updates, MFA, and approved security controls required by IT/Security.
Protect company and client data	Do not store client or confidential company data locally unless approved. Do not copy data into personal notes, screenshots, cloud storage, or consumer AI tools.
No unapproved AI apps or plug-ins	Do not install or use AI apps, browser extensions, desktop agents, or mobile tools that can access company data without approval.
Report loss or compromise	Immediately report lost, stolen, compromised, or suspicious devices to the IT Service Desk or Security Incident Hotline.
Allow business data removal	Company-managed data, apps, access tokens, and accounts may be remotely removed or wiped when required for security, employment changes, investigations, or loss of device.
Preserve evidence when directed	If an incident occurs, do not delete messages, prompts, logs, files, apps, or chat history unless instructed by Security or Legal/Compliance.
Follow offboarding procedures	Return or remove company data, revoke access, and cooperate with account/device cleanup during role changes or separation.

Company Rights and Controls for BYOD

- The company may deny, limit, suspend, or revoke personal device access if minimum security requirements are not met.
- The company may monitor company accounts, managed applications, access logs, security alerts, and data movement associated with business use.

- The company may remotely remove company-managed apps, accounts, tokens, certificates, and company data from the device.
- The company may require the device to be inspected or preserved when necessary for a legitimate security, legal, compliance, or client investigation, subject to applicable law and company procedure.
- The company may block use of personal devices for high-risk roles, privileged access, regulated data, or client environments where stronger controls are required.

Personal Device Prohibitions

- Do not use personal AI accounts to process company or client data.
- Do not forward company or client data to personal email, messaging, file storage, or note-taking tools for AI use.
- Do not screenshot, record, transcribe, or upload confidential information into consumer AI tools.
- Do not connect personal AI assistants to company email, calendar, file storage, ticketing, or collaboration systems without approval.
- Do not use jailbroken, rooted, unsupported, or unmanaged devices for business access.

13. Software Development, Automation, and Cybersecurity Use

AI-Assisted Development

- AI-generated code is not automatically approved, secure, licensed, or correct.
- Do not include secrets, tokens, proprietary client code, or restricted data in prompts unless the tool is approved for that data.
- Review code for security vulnerabilities, license concerns, data leakage, logic errors, performance issues, and maintainability.
- Use standard development controls, including peer review, testing, static analysis, dependency review, and change management.
- Document AI use when required for client deliverables, regulated systems, or internal quality procedures.
- Do not use AI-generated code in production or client environments without approval by the responsible owner.

AI Agents and Automations

Requirement	Details
Least privilege	AI agents must use accounts with only the permissions needed for the approved task. Privileged access requires additional approval.
Human approval gates	Human approval is required before agentic AI sends external messages, modifies client systems, deploys code, deletes records, or performs high-impact actions.
Logging	Inputs, outputs, actions, approvals, and errors must be logged where practical.
Change management	Automations that affect production or client systems must follow change management, testing, and rollback requirements.
Monitoring	Owners must monitor agent activity, failures, unexpected behavior, and misuse.
Kill switch	Business-critical agents should have a documented method to pause, disable, or revoke access quickly.

Cybersecurity Use

- AI may be used for authorized defensive security work, such as alert triage, incident summaries, detection engineering, vulnerability prioritization, and documentation.
- Do not use AI for unauthorized offensive actions, exploit development, phishing, credential harvesting, persistence, evasion, or social engineering.
- Security-sensitive data must be handled only in approved security tools and in accordance with client agreements and incident procedures.
- AI recommendations for security actions must be validated before execution.

14. Communications, Marketing, Sales, and Customer Support

External Communications

- AI may assist with drafts, but employees must review and approve final communications.
- Do not send AI-generated messages that are deceptive, misleading, inaccurate, or inconsistent with company commitments.
- Do not use AI to impersonate another person or organization without authorization and appropriate disclosure.
- Do not disclose confidential or client information in prompts or generated content.
- Escalate legal claims, security claims, compliance claims, and client commitments for review before distribution.

Sales and Marketing Claims

- All AI-assisted sales claims, case studies, testimonials, ROI statements, security claims, and performance claims must be substantiated.
- Do not create fake testimonials, fake reviews, fake customer references, or fake case studies.
- Do not use AI-generated images, voices, or videos in a way that suggests a real person, client, or event without approval.
- Client names, logos, and references require authorization under the applicable client agreement and company process.

Customer Support

- AI may assist support teams with suggested responses, summaries, and troubleshooting steps when the tool and data use are approved.
- AI must not independently close tickets, change priorities, issue commitments, perform changes, or send client-facing responses unless specifically approved.
- Support staff must validate technical instructions before providing them to clients or executing them.

MIS

15. Meeting Assistants, Voice, Images, Video, and Synthetic Media

Meeting Assistants and Transcription

- Use only approved meeting recording, transcription, and summarization tools for business meetings.
- Notify participants and obtain consent where required by law, contract, or company procedure before recording or transcribing.
- Do not use meeting assistants in meetings involving regulated data, legal privilege, HR matters, security incidents, M&A, executive strategy, or client confidential topics unless approved.
- Meeting summaries must be reviewed before being treated as official notes or distributed externally.
- Store transcripts, recordings, and summaries in approved systems and retain them according to records retention rules.

Synthetic Media and Deepfakes

- AI-generated images, audio, video, avatars, or voices must not be used to mislead or deceive.
- Do not generate or distribute synthetic media depicting employees, clients, vendors, or public persons without authorization.
- Label or disclose synthetic media when required by policy, law, contract, or context.
- Do not use synthetic media for harassment, discrimination, coercion, fraud, or reputational harm.

16. Vendor, Procurement, and Contract Requirements

AI tools and AI-enabled features must follow the company vendor management process before business use. Procurement must not rely only on product marketing claims.

Review Area	Questions to Answer
Vendor terms	Who owns prompts, uploaded files, and outputs? Can the vendor use data to train models? Can terms change without notice?

Review Area	Questions to Answer
Security	What encryption, access control, logging, vulnerability management, incident notification, and tenant isolation controls exist?
Privacy and data protection	What personal data is processed? Where is data stored? Who are subprocessors? What deletion and retention controls exist?
Compliance	Does the tool support applicable client, industry, contractual, and regulatory obligations?
Intellectual property	Are outputs protected? Are there license restrictions? Can outputs create infringement risk?
Data residency and retention	Where will data be processed and stored? How long are prompts, files, and outputs retained?
Model behavior	What are known limitations, hallucination risks, bias risks, and guardrails?
Operational resilience	What happens during outages, vendor incidents, model changes, or service termination?

Contract Expectations

- Confidentiality and data protection obligations appropriate to the data processed.
- Restrictions on vendor use of company or client data for model training unless explicitly approved.
- Security controls, breach notification, audit rights, or assessment rights appropriate to risk.
- Data deletion, export, retention, and offboarding terms.
- Subprocessor disclosure and change notification where relevant.
- Service levels, support, availability, and change notification for critical tools.

MIS

17. Logging, Monitoring, Records, and Retention

Company use of AI may be logged, monitored, reviewed, and audited to protect company and client interests, ensure compliance, and investigate incidents.

Monitoring May Include

- Access to approved AI systems, including user, timestamp, tool, and administrative activity.
- Prompts, files, outputs, and actions where supported by the tool and permitted by law and contract.
- Data movement between AI tools and company systems.
- Use of personal devices only to the extent associated with company accounts, managed apps, business access, or security-relevant activity.
- Agentic actions, approvals, API calls, changes, messages, tickets, and execution logs.

Records and Retention

- Final work product must be saved in approved company systems, not only in AI chat history.
- AI-generated or AI-assisted records must follow the same retention requirements as equivalent non-AI records.
- Do not delete prompts, outputs, logs, or files related to a suspected incident, investigation, legal hold, client issue, or compliance review.
- AI chat history is not an approved system of record unless explicitly designated by the company.

18. Security Incidents and Data Exposure Response

FIRST RESPONSE

Stop using the tool, preserve evidence, and contact the Security Incident Hotline immediately if sensitive data may have been exposed or an AI system acted unexpectedly.

Examples of AI Incidents

- Sensitive data was entered into an unapproved AI system.
- An AI tool retained, displayed, leaked, or returned data that should not be available.
- Credentials, tokens, private keys, secrets, or client identifiers were entered into AI.

- An AI agent changed a system, sent a message, deleted data, or executed a workflow without required approval.
- AI output caused an incorrect client recommendation, production issue, security exposure, or contractual concern.
- A suspicious AI plug-in, browser extension, or mobile app accessed company data.
- AI-generated content created reputational, legal, HR, client, or regulatory risk.

What to Do Immediately

- Stop entering additional data into the AI system.
- Do not delete prompts, outputs, files, logs, browser history, chat history, or tool records unless instructed by Security or Legal/Compliance.
- Capture relevant details: tool name, account used, date/time, data entered, output received, people involved, client affected, and any actions taken.
- Contact the Security Incident Hotline or IT Service Desk using the escalation table in this policy.
- Notify your manager and client account owner if client data or client systems may be involved.
- Follow instructions from Security, Legal/Compliance, and Incident Response leadership.

Response Ownership

- Security leads technical investigation, containment, and evidence preservation.
- Legal/Compliance determines notification, contractual, and regulatory obligations.
- Client account leadership coordinates client communication when approved.
- IT supports access revocation, logging, device actions, and system containment.
- Employees must cooperate and provide accurate information promptly.

19. Training, Awareness, and Enforcement

Training Requirements

- Employees must complete AI usage and data handling training before using approved AI systems for business where required by role.
- Privileged users, developers, security staff, and users of agentic AI may require additional role-specific training.
- Training must cover approved tools, prohibited data, human review, client restrictions, personal device rules, and incident reporting.
- Managers must ensure their teams understand permitted and prohibited AI use cases.

Enforcement

- Violations may result in coaching, mandatory retraining, access restriction, disciplinary action, termination, contract remedies, or legal action, depending on severity.
- The company may revoke access to AI tools or systems if a user violates this policy or presents unacceptable risk.
- Intentional misuse, data exposure, credential disclosure, client harm, deception, harassment, or security bypass may be treated as severe misconduct.

20. Exceptions and Review

Exception Process

- Exceptions must be requested in writing before non-standard AI use occurs.
- Exception requests must include business justification, data involved, tool/vendor, users, duration, risks, and compensating controls.
- Security, Legal/Compliance, business owner, and data owner must approve exceptions appropriate to risk.
- Exceptions must have an expiration date and must be reviewed before renewal.
- Emergency exceptions must be documented as soon as practical after approval.

Policy Review

- This policy must be reviewed at least annually.
- Review is also required after material AI vendor changes, incidents, regulatory changes, client requirement changes, or major changes to company AI use.
- The AI Policy Owner is responsible for coordinating review and distributing approved updates.

MIS

Appendix A - Quick Reference: Do and Do Not

Do	Do Not
Use approved AI tools for approved business purposes.	Do not use personal AI accounts for company or client data.
Ask IT/Security before using a new AI tool, plug-in, or automation.	Do not paste secrets, credentials, keys, or tokens into AI.
Minimize and mask data where practical.	Do not enter client or regulated data unless approved for that tool and use case.
Validate AI outputs before using them.	Do not trust AI output as accurate, current, or secure without review.
Follow client contracts and restrictions.	Do not use one client's data to support another client.
Report suspected AI data exposure immediately.	Do not delete evidence after a potential incident.
Use human approval gates for agentic AI.	Do not allow AI to make client-impacting changes without approval.
Review AI-generated code for security, licensing, and functionality.	Do not deploy AI-generated code without testing and change approval.

Appendix B - AI Data Entry Decision Tree

1. Is the AI tool listed in the Approved AI Systems Register for this use case? If no, stop and request approval.
2. Does the prompt include credentials, tokens, secrets, or private keys? If yes, stop and report if already entered.
3. Does the prompt include client, confidential, regulated, HR, financial, security-sensitive, or proprietary data? If yes, confirm the tool is approved for that data and purpose.

4. Does a client contract, policy, or statement of work restrict AI use? If yes or unknown, consult the client account owner, Security, or Legal/Compliance.
5. Can the data be minimized, anonymized, or masked? If yes, do that before use.
6. Will the AI output affect a client, production system, employee, external communication, legal/compliance matter, or security decision? If yes, require human review and documented approval.
7. Save final approved work in the correct system of record.

Appendix C - AI Tool or Use Case Request Form

Field	Response
Requester / Department	[Insert requester and department]
Tool or Vendor Name	[Insert name]
Business Use Case	[Describe what the AI tool will do]
Users / Roles	[List users, teams, or roles needing access]
Data Types Involved	[Public / Internal / Confidential / Client / Regulated / Security Sensitive]
Client Data Involved?	[Yes / No / Unknown. If yes, identify clients and contract restrictions.]
Will the AI Tool Train on Input Data?	[Yes / No / Unknown. Attach vendor documentation.]
Retention / Deletion Controls	[Describe how prompts, files, and outputs are stored and deleted]
Integrations / Permissions	[Systems connected, permissions requested, API scopes]
Agentic Actions?	[Can the tool send, change, delete, execute, deploy, or call APIs?]
Security Controls	[SSO, MFA, logs, encryption, admin controls, tenant isolation]

Field	Response
Risk Level	[Low / Medium / High / Critical]
Required Approvals	[Business Owner / IT / Security / Legal / Compliance / Data Owner / Client]
Decision	[Approved / Approved with restrictions / Denied / More information needed]
Expiration or Review Date	[Insert date]

Appendix D - Approved AI Systems Register Template

Tool Name	Owner	Approved Uses	Permitted Data	Restrictions	Review Date
[Tool 1]	[Owner]	[Use cases]	[Data classes]	[Key limits]	[Date]
[Tool 2]	[Owner]	[Use cases]	[Data classes]	[Key limits]	[Date]
[Tool 3]	[Owner]	[Use cases]	[Data classes]	[Key limits]	[Date]

Appendix E - Personal Device AI Use Acknowledgment

Complete this acknowledgment for users authorized to access approved AI systems or company data from a personally owned device.

Acknowledgment Item	Employee Initials
I understand that company and client data accessed on my personal device remains subject to company policy.	_____
I will use only approved company accounts and approved AI tools for business purposes.	_____
I will not enter company, client, regulated, or security-sensitive data into personal or unapproved AI tools.	_____
I will maintain required device security controls, including screen lock, updates, encryption, and MFA where required.	_____
I will report a lost, stolen, or compromised device immediately.	_____
I understand company-managed business data, apps, tokens, and access may be removed or disabled for security, employment, legal, or compliance reasons.	_____
I understand the company may monitor company accounts, managed applications, and security-relevant access associated with business use.	_____

Employee Name: _____ **Date:** _____

Employee Signature: _____

Appendix F - Employee Acknowledgment

By signing below, I acknowledge that I have received, read, and understand the AI Usage Policy. I agree to follow the policy and related company policies. I understand that violations may result in access restriction, disciplinary action, or other consequences.

Employee Name: _____

Title / Department: _____

Signature: _____ **Date:** _____

Manager / Witness: _____ **Date:** _____

Appendix G - Reference Alignment

This policy is designed to align generally with widely used AI governance, cybersecurity, consumer protection, and management system principles. These references are informational and do not replace legal advice, client contract requirements, or company-specific risk decisions.

NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0): *https://www.nist.gov/itl/ai-risk-management-framework*

NIST Cybersecurity Framework (CSF) 2.0: *https://www.nist.gov/cyberframework*

ISO/IEC 42001:2023 Artificial Intelligence Management System: *https://www.iso.org/standard/42001*

Federal Trade Commission Artificial Intelligence resources and enforcement materials: *https://www.ftc.gov/industry/technology/artificial-intelligence*