ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Acceptable Usage of AI Code Generation Tools Policy

Document ID:	AG-ISMS-POL-AICODE
Version Number:	1.0
Issue Date:	08, August, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Acceptable Usage of AI Code Generation Tools (the "Policy") is part of the AI governance policies framework. It outlines key guidelines to offer clear direction to Allegis Group and its operating companies' (OPCOs) developers on when and how AI-based coding assistants (refer to section 3) can be utilized to enhance productivity, and when their use is prohibited. This policy strikes a balance between the efficiency gains of these tools and compliance with client contracts, intellectual property rules, and security standards.

This applies to all developers (employees, contractors, and third-party staff) working on Allegis Group & its operating companies' software projects, who must only use company-provided assets. Violations (e.g., using unapproved AI tools or misusing approved ones) may result in disciplinary action or loss of access.

2 PRODUCTIVITY TOOLS – DEFINITION, BENEFITS, AND APPROVED

(1) **Definition:** These are AI-powered coding assistants that can generate or suggest code, functions, or other development outputs. These tools use large language models trained on source code to predict and propose code snippets based on context.

(2) **Benefits:** Used properly, these tools can accelerate development and reduce repetitive work for developers. They help by autocompleting boilerplate code, suggesting algorithms or syntax, writing documentation drafts, and even creating unit tests. Developers can then focus more on complex logic and design:
   a. **Speed:** Faster coding of routine sections, reducing development time.
   b. **Quality Assistance:** AI can suggest best practices or catch simple errors in real-time.
   c. **Learning:** Developers can learn new patterns or syntax from AI suggestions as they code.
   d. **Focus:** Engineers spend less time on trivial or boilerplate code and more on critical architecture and problem-solving.

(3) **Approved:** As of now, Allegis Group approves GitHub Copilot (Enterprise Plan), Salesforce Agentforce for developers, and Microsoft Copilot for use on projects that are not restricted by client policies. The user should have a license in Allegis's group enterprise tenant and should not use the free version provided by Microsoft.
   a. **GitHub Copilot (Business/Enterprise Plan):** AI code assistant integrated in Integrated Development Environments (IDEs) like Visual Studio Code. The user should have a GitHub Copilot license in the Allegis Groups enterprise GitHub tenant (https://github.com/enterprises/allegis-group) and should not use the free version provided by Microsoft.
   b. **Microsoft Copilot (e.g., in GitHub, Visual Studio, Teams, Web):** Enterprise AI assistant features in Microsoft platforms. The user should have a license in the Allegis Groups enterprise tenant and must be logged in. We recommend using the work tab when possible.
   c. **Salesforce Agentforce for Developers:** The Agentforce for Developers extension is an AI-powered developer tool that's available as an easy-to-install Visual Studio Code extension built using CodeGen and SFR Model, secure,

custom AI models from Salesforce.

(4) **Exception:**

a. **Pilot Applications:** If an application is custom-developed in-house by an OPCO for code generation, it must undergo approval by the ARB and AI council (Allegis & OPCO) before being released as a POC or to a broader audience.

- Pilot - Deployed in a production environment with a small user group and involves production data.

b. **New 3rd party tool:** If an OPCO wishes to implement a new code generation tool, it must undergo the TPRM, ARB, and AI Council (Allegis & OPCO) approval process before proceeding to POC or wider release.

3 General Guidelines for Usage

CRITICAL REMINDER: When in doubt, always choose the more restrictive option. Customer contracts and security requirements take precedence over productivity gains. Contact your manager/ your information security team for any unclear situations.

SL.No	Guidelines	Description
1.	Use Only Allegis Accounts	User should always login to the Allegis Group Tenant. For example, log into GitHub Copilot/Salesforce Agentforce with your Allegis corporate account under our enterprise license. Do not use personal subscriptions or any tool outside of IT's oversight. Enterprise settings (like license filtering to avoid verbatim use of public code) must remain enabled.
2.	Check Client Policies First	Always verify the client or project's policy on AI usage. If a client's contract forbids AI-generated code or unapproved tools, you must not even use the Allegis approved AI assistant tools on that project. If the client permits or encourages AI usage, you may use it only in accordance with this policy's controls. When in doubt, consult the project manager or legal team about contract restrictions before enabling AI assistance.
3.	Federal Data /Projects	The enterprise tenant should not be used for federal government projects and no data/information should be added to the approved AI tools. For additional information, contact your manager.
4.	State Government Data / Project	Before using Allegis approved AI tools for a state government project, contact your manager and get written approval before using AI tools.
5.	No Confidential Data in Prompts	Never input sensitive or proprietary information into an AI tool that isn't explicitly cleared for such data. Even though our approved AI tools are configured not to retain or share your code externally, avoid exposing any client/Allegis group confidential data, passwords, or personal data in your prompts. For instance, don't paste a client's code or data schema

		into an external AI chat to get help. Only use AI within integrated development environments (IDEs) that are approved, where your code stays within our environment.
6.	Treat AI Suggestions as Drafts (Review Everything)	You are responsible for every line of code you accept from an AI. AI suggestions are often helpful starting points, but they may be incorrect, inefficient, or not fully aligned with requirements. Always review, test, and understand the code that AI tools suggest. If you do not understand a suggestion, do not use it. Never blindly accept AI output-it must be evaluated and edited by a human developer.
7.	Maintain Coding Standards	Ensure AI-generated code adheres to our quality and style standards. This includes proper naming conventions, error handling, performance considerations, and alignment with project architecture. If the AI tools suggestion doesn't follow our standards (e.g., poor naming or outdated approach), refactor it accordingly. The presence of AI does not excuse us from writing clean, maintainable code.
8.	Document or Flag Significant AI Contributions	While not always required, it's good practice to add comments or notes in commit messages when a significant piece of code was AI-generated. For example, "Used Copilot/Agentforce to draft the initial version of this module, then refactored." This transparency can help in future maintenance and in case any legal questions arise about code origin. It is also recommended to add adequate comments (e.g. "code generated by AI tool") in the line of code/section where it is used.

4 ALLOWED USE – EXAMPLE SCENARIOS

Below are examples of scenarios where the use of AI tools is permitted under this policy. In all cases, assume that no client-specific rule prohibits AI use and that all general guidelines and controls are followed.

Allowed Scenario	**Why It's Allowed / How to Use AI Here**
Internal Proof-of-Concept Project (no external client involved) e.g., Building an internal tool or automation script.	✅ Allowed. Since it's an internal project, there are no client restrictions. Using AI tools can speed up development (for instance, suggesting boilerplate code or API call usage). Ensure you still review all AI-suggested code and that no sensitive internal logic is exposed outside. This scenario is ideal for AI assistance because the risk is relatively low and contained.

Client Project – AI Permitted e.g., Client's contract explicitly allows or even encourages AI tool usage, and the tool has been reviewed and approved by Allegis and OPCOs AI Council.	✅ Allowed, with oversight. You may use AI tools to assist coding on this project since the client, Allegis and OPCO has approved it. Stick to company-approved AI tools and adhere to our controls (no sensitive data in prompts, thorough reviews). It's wise to inform the team (and the client, if appropriate) that AI assistance is being used to maintain transparency. The code still must meet all project standards and go through normal QA.
Generating Unit Tests e.g., After writing a new feature, using Copilot/Agentforce to generate unit test skeletons.	✅ Allowed. Writing tests is often repetitive – AI tools can suggest test cases or boilerplate for testing frameworks. This usage is safe because it's based on code you wrote and common patterns. You must verify that tests are meaningful and adjust any assertions or edge cases, but AI can significantly speed up creating a broad suite of tests.
Common Boilerplate or Utility Code e.g., Getting a quick snippet for a common task (file parsing, date formatting).	✅ Allowed. For well-understood, generic code (standard algorithms or language-specific boilerplate), AI tools can save time. For example, it might suggest a quick sort implementation or a date formatting function. There's low risk as this is common knowledge territory, not proprietary. Still, test that the snippet works as expected in your context and conforms to any performance needs.
Learning a New Technology e.g., Using AI for examples while working in a new framework (Salesforce Apex, etc.).	✅ Allowed. If you're ramping up on a new language or framework, you can use AI tools to suggest examples or remind syntax. This helps you learn faster. Ensure that any code you use is adapted to your actual solution. Essentially, AI can act like an intelligent tutor or reference manual. Just be cautious not to copy an entire complex snippet blindly; use it to understand the pattern, then implement with your data/requirements.

5 RESTRICTED/PROHIBITED USE – EXAMPLE SCENARIOS

Below are scenarios where AI tool usage is prohibited or should be avoided. These examples highlight situations of high risk or explicit restriction:

Prohibited Scenario	**Why It's Not Allowed (or Requires Caution)**
Client-Restricted Project e.g., Client's contract forbids AI or unapproved tools for their code.	❌ Not allowed. This is non-negotiable. If a client says "no AI-assisted development," we must comply 100%. Using AI tools on such a project would violate the contract and could lead to serious legal and business repercussions. In this case, you should disable AI tools in IDEs or not generate code through any form of AI for that project and write code manually. Document that AI was not used due to client restrictions, if needed.

Highly Confidential or Proprietary Code or Federal or State government projects e.g., Developing a secret algorithm or system that is a competitive differentiator.	❌ Not allowed for code generation. Core intellectual property or sensitive algorithms should not be exposed to AI suggestions. Even if using approved tools, there's some risk in letting AI see the code, and we want the design to remain strictly in-house. Also, AI might not handle highly specialized logic correctly. It's better for our experts to write this code without AI to ensure secrecy and correctness.
Blind Copy-Paste from AI or Web e.g., Accepting a large code snippet from AI tools or public websites/blogs without understanding or attribution.	❌ Not allowed. Our policy explicitly forbids blindly copy-pasting code from third-party sources. If AI tool suggests a big chunk of code (especially if it looks generic or from a known library), you must not just drop it in. It could be copyrighted or incompatible with our project. Instead, use it as insight: write your own implementation or verify the source license and attribution requirements. Failing to do so can introduce legal and security issues.
Using Unapproved AI Services e.g., Trying out a new AI coding plugin or an online AI tool that IT hasn't vetted.	❌ Not allowed. All AI coding tools must be approved. Using an unapproved tool (even if it's free or popular) is risky: it might upload code externally or produce poor results. For example, do not paste code into a non-approved tool or a random website for debugging help. If you think a tool is valuable, suggest it to our AI governance team for evaluation rather than using it clandestinely.
Automated Client-Facing Content e.g., Letting AI generate a code comment or documentation that goes directly to a client without human review.	⚠️ Not allowed without review. While using AI to draft documentation or emails is not strictly "coding," it's related. We never want to present raw AI-generated text to clients without human revision. If AI tool helps write a design doc or an explanatory comment, ensure a person edits it for accuracy, tone, and clarity before sharing. This avoids misinformation or an impersonal feel in deliverables. In short, AI can draft, but a human must approve anything that leaves our company.

Summary of Prohibited Use: Do NOT use AI tools when a client disallows it, when dealing with highly sensitive code, or when you cannot ensure the integrity of the output. If the situation is borderline or you're unsure, err on the side of caution and skip the AI assistance. It's better to take a bit longer coding by hand than to risk a breach of contract or a security lapse. When necessary, seek guidance from your manager or the AI Center of Excellence.

6 Controls and Monitoring to Ensure Compliance

Even in allowed scenarios, strict controls must be followed to mitigate risks:

(1) **Enterprise Configuration & Settings:** Always use AI tools in their enterprise-configured mode. For GitHub Copilot Enterprise, our IT admins have enabled settings like "Block suggestions matching public code" (to prevent plagiarism of open-source code) and ensured our private code stays private. Do not attempt to change or circumvent these settings. Similarly, use AI tool features only within our protected environment/company approved assets.

Note: The enterprise administrator will regularly adjust the configurations, which may result in the reduction of some features (e.g., multiple LLMs), potentially due to the impact

of our security guidelines or cost overruns.

(2) **No Direct Third-Party Code Ingestion:** As a rule, do not bring external code into our codebase without verification. AI tools may sometimes suggest code that appears to be from a shared library or an online example. If you recognize it (or it's longer than a few lines), double-check it. Use a web search to see if that exact code is publicly available. If it does and is licensed, you must comply with that license (which often means not using it unless it's a permissive license, such as MIT, and even then, attribution may be required). Prefer to have AI tools assist you in writing your 'own' version of the solution rather than copying verbatim. This way, we avoid any hidden licensing traps and ensure the code is tailored to our needs.

(3) **Code Reviews Flag AI-Generated Sections:** During peer code reviews, developers should highlight any significant AI-generated code in their commits or merge requests. This gives reviewers a heads-up to scrutinize that part closely. Reviewers will ask for clarifications on logic to ensure the author understands it. If a developer cannot confidently explain a piece of code that came from AI, that code should not remain. The team may decide to rewrite it from scratch if it's not well-understood. This practice keeps our code maintainable and knowledge shared.

(4) **Thorough Testing and QA:** AI-generated code must pass all the same tests and quality checks as handwritten code. Be extra vigilant: add more unit tests for complex code that AI tools contributed to, to catch edge cases. Run static analysis and security scans on all new code. For example, if Copilot helped generate an input parsing function, test it against any tricky inputs to ensure it's secure against injections or errors. Your QA team should be aware when AI is used so that they can focus on those areas during testing.

(5) **Code Security Scanning:** For projects hosted in Allegis Group's production environment (Azure/AWS/Google/Salesforce/Fusion/Snowflake, etc.), it is mandatory to run a code scan using Allegis Group's enterprise code scanning tools, such as CheckMarx or SonarQube. Code security scanning is required for customer projects if AI tools are used. Contact your manager or client partner for more information and to ensure that code scanning is completed before releasing the code. The code scanning process incurs a cost. For more details about CheckMarx, contact the Infosec team. For SonarQube, reach out to the relevant team.

(6) **Monitoring of AI Usage:** Allegis Group will monitor AI tool usage to some extent. Our enterprise systems can log usage statistics for AI tools (e.g., how often suggestions are accepted). This is to detect any misuse, such as over-reliance or potential data leaks. We do not read your code logs to micromanage, but if, for example, a large portion of code is auto-completed without edits, it may trigger a review to ensure compliance. Assume that nothing done with company tools is completely private – use AI responsibly, in line with this policy, at all times.

(7) **Training and Awareness:** Ensure that all users have completed Allegis Group's AI

training modules (https://degreed.com/plan/3471653).

7 Security & Compliance Checklist

Before Using AI Tools		After Code Generation	
☑	Check customer contract for AI restrictions	☑	Conduct peer code review
☑	Verify project security classification	☑	Run code security scanning tools
☑	Obtain necessary approvals	☑	Test generated code thoroughly
☑	Review data sensitivity level	☑	Document AI tool usage
☑	Confirm compliance requirements	☑	Update version control with proper tags
☑	3rd party risk management (TPRM) approval		
☑	Allegis & OPCO AI Council		

CRITICAL REMINDER: When in doubt, always choose the more restrictive option. Customer contracts and security requirements take precedence over productivity gains. Contact your manager/ your information security team for any unclear situations.

8 References

- Allegis Group – Policies and Procedures
  https://allegisintranet--simpplr.vf.force.com/apex/simpplr__app?u=/site/a143t00000Z5r8NAAR/dashboard

9 Contact Information

AI COE	AI_CoE_EA@allegisgroup.com
Information Security	corp_infosecoffice@allegisgroup.com

10 Document Information

Document Name	Acceptable Usage of AI Code Generation Tools Policy
Issue Date	08 August 2025
Next Review Date	1 January 2026
Author(s)	Sudhish Chemmur
Maintainer	Henry Fieglein
Owner	Pervez Nadeem

11 Version History

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Aug 8, 2025	First version of policy issued

12 Reviewers

AI COE	Wen Ji, Henry Fieglein, Sudhish Chemmur
Information Security	Tim McGee, Ramana Sivarchaka
Actalent	Pramad Nallari, Erik Wise

TGS	Roger Mazzolani, Beth Tomsic
AI Execution Champions	Monthly Meeting Cadence (07/24/2025)
Microsoft	Alex Williamson, Michele Thompson (Github SME)

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Artificial Intelligence ("AI") Policy

Document ID:	AG-ISMS-POL-AI
Version Number:	2.5
Issue Date:	30, June, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Artificial Intelligence ("AI") Policy (the "Policy"), forming an integral part of the Allegis Group Information Security Policies Framework, delineates our governance concerning Artificial Intelligence, including Generative AI or "GenAI" (hereinafter collectively referred to as "Artificial Intelligence" or "AI"). Allegis Group endorses the adoption of technologies that enhance work processes, boost productivity, and improve efficiency. Our mission with AI is to strategically integrate its capabilities into our business operations to propel innovation, efficiency, growth, and resilience while upholding secure and high-quality data practices and adhering to our responsible AI principles. We acknowledge that without the implementation of appropriate controls, the use of AI may lead to unethical, unsafe, or unlawful outcomes. This Policy establishes the governance framework for incorporating AI technologies within the company, ensuring data protection, security, and quality.

This Policy applies to the internal use of AI by all Company Personnel, regardless of role. Any Company Personnel whose primary job involves working with AI, whether for internal use or to provide products and services to clients, are subject to this Policy as well as any additional procedures and guidelines regarding the responsible development, use, and deployment of AI that are provided specific to their role. Additionally, external contractors who utilize AI in their work for the Company are also required to adhere to this Policy and any pertinent guidelines. Internal employees will play a critical oversight role, ensuring that external contractors comply with the established standards and practices for responsible AI usage.

This Policy outlines the Company's governance and principles for AI use, including both permitted and prohibited applications of AI. It specifically addresses current tools like generative AI (e.g., DALL-E, Midjourney), virtual assistants (e.g., ChatGPT, Microsoft Copilot), agentic AI (e.g., Salesforce Agentforce, Microsoft Copilot Studio), and artificial general intelligence (e.g., OpenAI Strawberry). However, this Policy is designed to be comprehensive enough to include any emerging AI technologies that may be developed in the future. While these AI tools are impressive and popular, they pose significant privacy, security, accuracy, and intellectual property risks. Compliance with this Policy ensures our AI use is safe, trustworthy, and lawful, adaptable to new AI innovations as they arise.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- All Company Personnel are expected to cooperate in the investigation; and

- Retaliation towards those who report incidents and violations of this Policy in good faith or cooperate in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section shall, for all purposes of this Policy, have the meanings specified as follows:

(1) "Artificial Intelligence" or "AI" is a broad term used to describe an engineered system that uses various computational techniques to perform or automate tasks. This may include techniques, such as machine learning, where machines learn from experience, adjusting to new input data and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making (as defined under Article 22 of the Australian Privacy Act 1988 and New Zealand Privacy Act 2020). Examples of AI include, without limitation, machine learning models, chat bots and Generative AI.

(2) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(3) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(4) "**Deepfake**" means audiovisual content that has been altered or manipulated using AI techniques. Deepfakes can be used to spread misinformation and disinformation. Other terms used to describe media that have been synthetically generated and/or manipulated include shallow/cheap fakes and computer-generated imagery (CGI).

(5) "European Sensitive Personal Data" means information collected from or about individuals in Europe (collectively "Europe" for purposes of this Policy refers to European Economic Area or EEA countries, the Australia and New Zealand, and Switzerland) relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, as well as data concerning health or data concerning a person's sex life or sexual orientation. In some EU member states, it may also include information about a person's criminal convictions.

(6) "**Generative AI**" or "**GenAI**" means the class of AI models that emulate the structure and characteristics of input data received through a prompt in order to generate derived synthetic content that can include images (i.e. Dall-E, Stable Diffusion, Midjourney) videos (i.e. Synthesia), audio (i.e., text, code and other digital content), etc. ChatGPT is the most well-known example, but other examples include Microsoft Copilot, Salesforce Agentforce, GitHub Copilot, DeepSeek, Stable Diffusion and Dall-E. GenAI tools are trained on large amounts of data, often sourced from the Internet, from which they spot patterns and learn to make predictions (e.g. "what word/pixel should come next"). They can use this learning to generate new content that is similar in style and structure to the data on which they have been trained. For example, a GenAI tool could be trained on a large number of books and articles and then be used to generate new sentences or paragraphs which are similar in style and tone to the

texts on which it was trained. Similarly, a GenAI image model could be trained on a large dataset of images and then be used to generate new images that are similar in style and content to the original dataset.

(7) "**Agentic AI**" or "**Virtual Agents**" refers to a class of artificial intelligence models capable of making decisions and taking actions autonomously, based on input data and pre-defined objectives. These models simulate intelligent behavior by processing vast amounts of information, learning from patterns, and executing tasks without direct human intervention. Think of it like a very smart robot or computer program that can understand what needs to be done and then do it, such as a virtual assistant that helps customers or a self-driving car. While these tools can make our work easier and more efficient, it's important to use them responsibly and in line with the laws and company policies.

(8) "**Information Security Policies Framework"** means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(9) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(10) "**Sensitive Personal Data**" means collectively European Sensitive Personal Data, any type of Personal Data that is considered "sensitive" data under applicable data protection law and for all individuals regardless of applicable data protection law, includes health data, biometric data, genetic data, an individual's account log-in, financial account, debit card, or credit card number when in combination with any required security or access code, password, or credentials allowing access to an account, immigration and citizenship status, and social security numbers, driver's license numbers, or other state/national identification numbers and state/national identity documentation (such as passports).

4 SCOPE

The target audience of this Policy is Company Personnel. Any Company Personnel must follow this Policy where they operate at a Company facility, when accessing any Company systems or networks (including, for example, when working from home or other remote location), or when they otherwise have access to Company Personal Data. Any Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to any additional policies provided to the Company Personnel by that third party (the more restrictive policy applies). Any Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as, such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 AI MISSION AND PRINCIPLES

The Company's AI mission is to harness the power of AI to support and drive company innovation, efficiency and growth through integration into our business processes and strategy while following our responsible AI principles. The Company adheres to the following AI Principles which guide our development, use and deployment of AI:

(1) **Fairness and Bias Detection** – Models and AI systems should be fair and free from bias.
(2) **Safety and Security** – Models and AI systems should be resilient, secure and safe throughout their entire lifecycle.
(3) **Accountability** –Someone must be accountable for the functioning of AI systems.
(4) **Explainability and Transparency** – AI systems should provide meaningful information and be transparent and explainable to end users.
(5) **Privacy** – Individual data privacy and data protection laws must be respected.
(6) **Validity and Reliability** - AI systems should perform reliably and as expected.

5.2 COMPANY USE OF AI - RISKS

As a counterbalance to the myriad benefits of AI, the Company recognizes that AI technologies are still being refined, are known to produce inaccurate or distorted information, and that the use of AI can create significant risks for the Company. This Policy aims to minimize the likelihood of risk of those concerns arising. Failure to comply with this Policy may result in harm to our Company Personnel, our customers, and members of society, and could cause legal and/or reputational risks to Allegis Group.

Some of the key concerns that can arise from the use of AI include:

(1) **Bias**: AI tools are only as unbiased as the data on which they are trained and the AI models leveraged, namely the methods in which they are tuned. If the training data contains biased or discriminatory content, the AI model may also produce biased or discriminatory content. Many AI tools are trained on data sourced from the Internet, which contains a lot of biased content (including gender-biased content, and content that can be discriminatory against religious beliefs, racial or ethnic origin, and sexual orientation, among others). Similarly, AI models rely on data that can have bias issues. Additionally, AI models that rely on humans to validate and/or tune models can introduce bias. Finally, the users of the AI, namely those writing prompts or tags which drive the results of the AI, can intentionally skew those inputs to achieve a desired results/answer thereby creating bias.
(2) **Disinformation and Deepfakes**: AI can be used to create content (such as text, imagery, audio or video) that, while it appears realistic and accurate, may be fake. This can be the result of AI "hallucinations" (where the AI appears to "make up" information) or because the AI has been trained on false data. Fake content, such as fake news or Deepfakes, can be used to spread misinformation or manipulate public opinion.
(3) Privacy: Personal Data may have been included within an AI tool's training data, and this is particularly likely where the AI tool has been trained on publicly-available data from the Internet. Consequently, the AI tool may generate content that violates a person's privacy – for example, by including private information about them in a generated response. Further,

because AI requires prompts in order to provide a response, you must be careful to not put Personal Data into the prompt since doing so may violate our Privacy Notice issued under the Australia and New Zealand General Data Protection Regulation (Australian Privacy Act 1988 and New Zealand Privacy Act 2020) and Australian Privacy Principles and New Zealand Information Privacy Principles to individuals for how we are permitted to use their Personal Data and for the reasons mentioned under Confidentiality below because the Personal Data may be leaked in responses to others. In developing AI models, it's critical to assess whether the use of Personal Data is proper under applicable data protection laws.

(4) Confidentiality: AI tools may learn from the prompts, data, and behaviour of the users interacting with them. If you enter commercially-sensitive or confidential information into an AI tool (such as information about our Company's customers), the AI may learn this information and leak it within responses given to other users from other organizations. Once an AI tool has "learned" information, it is very difficult to subsequently make it "forget" that information. Entering such information into AI tools may violate our policies against the disclosure of trade secret information and/or agreements we have entered into with other organizations that require us to keep their information confidential.

(5) Intellectual property: Material that is protected by intellectual property laws may also have been included within an AI tool's training data. Consequently, there are also concerns that AI can be used to create content which infringes on the intellectual property rights of others (for example, by including material that is protected by copyright (as governed by the Copyright Act 1968 (Cth) and New Zealand Copyright Act 1994) or under trademark (as governed by Australian and New Zealand intellectual property law) laws). There are similar concerns about whether or not content generated using AI is capable of intellectual property protections.

(6) **Safety and Security**: There are concerns about the safety risks of AI, particularly in areas such as self-driving vehicles or robotics, where AI could potentially create unsafe or dangerous situations (especially if it has received inadequate training, encounters "new" situations on which it was not trained or is forced to make a decision in harms-related scenarios, e.g. where a pedestrian steps in front of an autonomous vehicle making a collision inevitable and the AI has to decide who to save). AI can also be used in cybersecurity and fraud attacks, including, without limitation phishing campaigns.

ETHICS: THERE ARE BROADER ETHICAL CONCERNS ABOUT THE USE OF AI, PARTICULARLY IN AREAS SUCH AS MUSIC, ART OR LITERATURE, WHERE THERE ARE QUESTIONS ABOUT THE AUTHENTICITY AND ORIGINALITY OF THE CONTENT CREATED BY AI.

5.3 AI GOVERNANCE AND TRAINING

The Company invests in the reasonable resources necessary to support a responsible AI governance program that encompasses strategic, tactical and operational areas. The AI Governance will align with other Company governance structures. The AI Governance will include the AI Center of Excellence staffed with full-time Company Personnel and an AI Governance steering committee with appropriate personnel from the following stakeholder groups: operating company business leads, AI/data science, data governance, privacy, information security, human resources, ethics, compliance and risk management, enterprise architecture, project management, legal and IS leadership to provide input on operational goals and the use of AI to achieve them. In addition, the Company will support the infrastructure necessary to promote AI best practices, provide AI data science teams across the Company with support, help with knowledge sharing and drive standardization across all

teams working on AI initiatives. This will include, without limitation, the development of standards and best practices, policies and procedures to implement responsible AI, the establishment and implementation of an AI risk assessment process (e.g., the NIST AI Risk Management Framework), the establishment of a centralized AI inventory, the use of outside advisors and auditors and the development of an AI training program.

The Company will ensure that all employees receive appropriate levels of training related to the use of AI commensurate with their roles in the organization.

5.4 DO'S AND DON'T'S OF AI AND GENAI

The following are Do's and Don't's regarding your use of AI:

DO	DON'T
Only Use Company-licensed AI For Company Data – Where the Company has communicated to you that you are approved to use an AI tool for specific use cases, you are limited to using the approved AI for those specific use cases and according to any specific rules given to you for the tool's use (e.g., rules regarding setting up an account). Any other use cases may include data for which the AI has not been vetted, or which would increase the AI Risk footprint of the company.	**Do Not Use Company Confidential Data or Personal Data for AI Training or Input It in AI Prompts –** Unless Legal has approved otherwise, the Company will always opt-out of providing our Company confidential data and Personal Data for training of AI, so you must not agree to allowing any AI tool to use such data for training, including any pre-training and fine tuning of AI Models. You also must not use any Company data or Personal Data (including Sensitive Personal Data) in the AI prompts. For Company data, this means you cannot include any Company data (including data the Company is protecting on behalf of its employees, customer, vendors and other business partners) that is categorized as Confidential, Highly Confidential or Restricted under our Information Classification Policy.
Business/Personal Use of AI Tools – Company licensed AI is provided mainly for legitimate business purposes and should only be used for personal or non-business reasons on a limited basis and within reasonable limits. Such personal or non-business use must be in compliance with all other Allegis Group policies and specifically the Information Security Policies Framework listed in section 11 below.	**Do Not Assume That Standalone Cloud AI Applications Create No Risk –** Because Standalone Cloud AI Application require hardware and network connectivity, there needs to be a level or scrutiny in how the vendor views and acts upon the security of the cloud environment. Even tools running in major cloud environment (Microsoft Azure, Google Cloud Platform, Amazon Web Services) can be compromised if the proper levels of security are not adhered. Varying attacks from prompt injection to network sniffing make the information and prompts that you provide to the service available to hackers who may then use that as an attack vector to you or Allegis Group.

	If you can access the application, then there are attack vectors for hackers.
Follow the Company's Request for Work Process – Regardless of how standalone an application may seem, it requires integration into IS systems from user access controls to firewalls requiring some work from the IS teams who need to be able to plan their activities. Further, the OpCo appointed IS leaders need to understand the capabilities offered to their user community. To ensure that appropriate reviews and planning has occurred prior to TPRM submittal, an RFW should be created and approved.	
Follow the Company's Procurement and TPRM Process – All third-party vendors must be vetted through the Company's Third-Party Risk Management ("TPRM") process so that issues such as privacy, security, enterprise architecture and other risk points can be assessed, inclusive of specific vetting regarding AI. You must make sure any vendors you engage go through this process and cooperate in providing input, assistance and support as needed during the process. This cooperation includes openness on the part of the vendor of the capabilities of the product. For instance, the extent to which users can, or cannot, restrict product capabilities using settings controlled by the Company. Remember that the TPRM process approves specific use cases, so your use is approved only to the extent of the approved use case through TPRM. Any products we purchase from third-party vendors must be used in accordance with any user manual or instructions issued by the third-party vendor as failure to do so may cause the Company additional liability. Make sure you have undergone any relevant training offered by the third-party vendor or the Company. However, if you feel the product's use in any way compromises the security of the Company or violates this Policy or any other Company policy, you should report that as an incident under this Policy.	**<u>DO Not</u> Use AI Tools to Seek Legal Advice on a Company Related Matter** or to address a Human Resources (HR) or Employee Relations (ER) issue or as a substitute for seeking appropriate counsel and guidance from your Operating Company's subject matter experts.
Be Constantly Mindful of the Risks – Any time you are using AI, remember each of the risks noted in Section 5.1 and weigh those risks	**<u>Do Not</u> Use Work Related Materials on Public AI services –** Everyone has their favorite tools and services. This also includes AI services. Because of the familiarity with the favorite

against the benefits of using the AI before choosing to proceed to use the AI.	service, it may seem better or easier than the company supplied AI capability. While this may seem or even be true, the company has gone to great lengths to vet the security and data privacy of the company selected capability. Further, the company has secured licenses that will protect the confidentiality of company data. Working on your personal or a public version of an AI service exposes any company data or ideas that you share there to data theft or use in AI model training.
Use Human Judgment and Be Accountable – Understand that AI tools may be useful but are not a substitute for human judgment and creativity. Also remember that AI tools are prone to "hallucinations", false answers or information that is stale, so you must carefully verify any responses for accuracy, completeness, reliability and safety and to ensure that it does not contain any material that is obscene, defamatory, hateful, or infringes any intellectual property rights. You are responsible and accountable for any AI content you choose to further use.	**Do Not Use For Automated Decisions -** You must not use AI tools for the purpose of making automated decisions either about individuals (for example, used to make decisions to recruit or not recruit candidates) or companies (for example, whether a company can submit candidates) without the involvement of the Global Privacy Office. The definition of automated decisions is complex and varies by jurisdiction. If you believe any AI tool you are using involves automated decisions, please contact the Global Privacy Office. Certain AI functions like categorizing emails or handling certain user requests may not seem like they fall into this category, but it is better to check with the AI CoE or Global Privacy Office before moving forward. •
Follow Company Policies and Procedures Regarding AI – The laws are evolving quickly in the area of AI. As the Company adapts to these ever-changing laws, our policies, guidelines and procedures will adapt to address these legal requirements. You must adhere to all AI related policies, guidelines and procedures and take any required AI training. This may include, for example, documenting risk assessments relating to the development of AI, labelling requirements for GenAI content, performing bias audits, and providing notices. You understand that the Company may monitor your interactions with AI websites for compliance with this Policy. For more information on monitoring, please see the Company's Workplace Monitoring Policy. Your use of AI is at all times subject to this Policy as well as the Company's Information Classification Policy, Information Security Policy, Workplace Monitoring Policy and the Acceptable Use of	**Do Not Use to Perform or Facilitate Dangerous, Illegal or Malicious Activities –** For example, and without limitation, do not use AI to: • generate content related to abuse or exploitation, hatred, harassment, bullying or violence; • discriminate against individuals on the basis of race, color, religion, sex, gender, national origin, age disability, marital status, sexual orientation or any other class protected under applicable law; • facilitate or encourage individuals to commit crimes; • promote or generate violent extremism or terrorist content; • promote or facilitate the generation or distribution of spam; • generate content for deceptive or fraudulent activities, scams, phishing or malware; or

Electronic Resources Policy as well as the Company's Employee Handbook and Code of Conduct.	"jail break" the functionality of an AI tool so that its safety features are overridden.
Attribute Output to AI – Where required by applicable law, clearly attribute any output used for approved work purposes to the AI application that created it through a footnote or other means visible to the recipient.	**Do Not Use to Generate Content to Misinform or Mislead** – For example, to generate forged documentation, to create Deepfake textual or audiovisual material or to make misleading claims of expertise.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 EXCEPTION HANDLING

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Acceptable Use of Electronic Resources Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Workplace Monitoring Policy

9 DOCUMENT INFORMATION

Document Name	Artificial Intelligence ("AI") Policy
Issue Date	30 June 2025
Next Review Date	1 January 2026
Author(s)	Henry Fieglein
Maintainer	Christen Grapes
Owner	Pervez Nadeem

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Jan 1, 2024	First version of policy issued
2.0	Jan 1, 2025	Annual review - Minor changes to the Incident Response and Scope section consistent with changes made to all other Information Security Program Framework policies; update to definition section to change “EU” to “Europe”; added more examples of Generative AI in definition section; updated AI Principles and added AI Mission statement; updated Company approved AI section to move from pilot to larger rollout of Microsoft Co-Pilot licenses; Updated approval for AI projects to AI COE instead of the Legal team as initial point of contact; changed Owner of Policy to Pervez Nadeem as the leader of the AI COE
2.5	Jun 30, 2025	Updates based on wider distribution of AI capabilities. Preparations for further AI capability availability.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Acceptable Use of Electronic Resources Policy

Document ID:	AG-ISMS-POL-ERP
Version Number:	14.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Acceptable Use of Electronic Resources Policy (the "Policy") is part of the Information Security Policies Framework and sets out important rules governing the use of Electronic Resources and Social Media, including the use of any of these on personal accounts through personal equipment or through other non-Company assets that connect to any Company systems or network or affect the Company in any way, whether intentional or not.

This Policy reflects the state of technology as of the date of its adoption; therefore, technological developments may exceed the literal text of this Policy.

This Policy also outlines the use of external or cloud services such as Dropbox, Gmail and Google Docs, Box.com, Salesforce, Amazon Web Services, and Azure.

The Company entity that is legally responsible for the processing of any Personal Data processed about you for the purposes of this Policy is the Company entity that employs or contracts with you.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them.

The Company needs your help in identifying those incidents and violations. An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(2) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(3) "**Electronic Resources**" means any (a) information technology equipment, devices or related equipment (such as servers, computers, laptops, desk phones, mobile phones, tablet PCs (e.g., iPad), thumb drives or other storage devices or multi-function printer/copier/scanner/fax machines); (b) electronic key fobs/cards; (c) internet and internet connections; (d) intranets; (e) network file shares (such as the Q:, S:, T:, U: or O: drives); (f) file sharing sites (such as Team Sites, OneDrive and SharePoint); (g) databases; (h) online subscriptions and services (such as WebEx or LinkedIn Recruiter); (i) applications, whether cloud or on-premise (such as Office 365, voice mail, PeopleSoft, Salesforce ("Connected") or Bullhorn); (j) wearable or 'nearable' devices or any equipment comprising the 'internet of things', and (k) CCTV and any other similar resources of any kind each of which are (i) supplied by the Company to you for use for work-related purposes or (ii) not supplied by the Company to you, but are either: (a) used by you to connect to any Company network or (b) used in a way that relates to the Company or your work for the Company, whether intended or not.

(4) "**European Sensitive Personal Data**" means information collected from or about individuals in Europe (collectively the "Europe" for purposes of this Policy refers to the EEA countries, the UK and Switzerland) relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, as well as data concerning health or data concerning a person's, sex life or sexual orientation. In some European member states, it may also include information about a person's criminal convictions.

(5) "**Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(6) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(7) "**Sensitive Personal Data**" means collectively European Sensitive Personal Data, any type of Personal Data that is considered "sensitive" data under applicable data protection law and for all individuals, regardless of applicable data protection law, includes health data, biometric data, genetic data, an individual's account log-in, financial account, debit card, or credit card number when in combination with any required security or access code, password, or credentials allowing access to an account, immigration and citizenship status and social security numbers, driver's license numbers, or other state/national identification numbers and state/national identity documentation (such as passports).

(8) "**Social Media**" means collectively forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as photos or videos), and without meaning to create an all-inclusive list, includes any of the following: Facebook (Meta), LinkedIn, X, TikTok, Pinterest, Instagram, YouTube, WeChat, WhatsApp, Snapchat, Tumblr, Reddit, Quora and Flickr and Company-maintained sites (such as Yammer, Viva Exchange and Microsoft Teams chat).

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote locations). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically

present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 PRINCIPLES REGARDING USE OF ELECTRONIC RESOURCES

A. Authorized Access.
Only authorized users must have access to Electronic Resources.

B. Compliance with Laws and Policies.
When using Electronic Resources, you must always comply with any applicable laws and regulations, this Policy and the supporting policies set forth in Section 8. This includes, without limitation, protecting Personal Data in compliance with applicable data protection and/or information security laws, and the Personal Data Protection Policy. If any legal claim is made for possession of, or access to, Electronic Resources, this must be referred to the Company's Legal department without delay.

C. Sensible Use.
Your use of Electronic Resources must be sensible and in such a manner that it does not interfere with the smooth and efficient running of the business. The Company reserves the right to alter this Policy at any time if this trust is abused.

D. Information Protection.
You must protect all information (including Restricted, Highly Confidential and Confidential information, as defined in the Company's Information Classification Policy and the Information Security Policy) owned by the Company and its licensees (for example, proprietary code) while such information is in the Company's custody.

E. Business/Personal Use.
The Electronic Resources are provided mainly for legitimate business purposes and should only be used for personal or non-business reasons on a limited basis and within reasonable limits.

5.2 UNACCEPTABLE USES OF ELECTRONIC RESOURCES

When using Electronic Resources, you must **NOT** engage in any of the following:

A. Abusive, Obscene or Discriminatory Use	B. Export Controls Violations	C. Illegal or Inappropriate Activity
D. Improper Disclosure of Confidential Information	E. Legal or Other Harm to Company or Others	F. Disruption/Damage or Unauthorized Access
G. Viruses	H. Social Networks/Websites – Violation of Terms of Use	I. Advertisement or Inappropriate Solicitation
J. Impersonation	K. Sending Email Without Consent, Where Required	L. Copyright Violation
M. Install Unauthorized Software	N. Fraud/Misleading Statements or Fraudulent Email Headers	O. Unauthorized Company Warranties, Guarantees, Representations or Contractual Commitments
P. Unapproved Wired Device Connections	Q. Unsecured Wireless Connections	R. Inappropriate Sharing of Electronic Resources
S. Sending Trivial/Unnecessary Emails	T. Improper Use of Another Person's Computer or Email/ Assumed Identity	U. Unsecure Sending, Storing or Providing Access to Sensitive Personal Data

For more details on each of the above, please see each item below.

A. Abusive, Obscene or Discriminatory Use

Using Electronic Resources in a way that is abusive, obscene, discriminatory, racist, harassing, derogatory, offensive or liable to cause embarrassment to the Company or others.

B. Export Controls Violation

Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. For example, this includes traveling outside of the United States with a laptop computer that is an Electronic Resource that contains such information.

C. Illegal or Inappropriate Activity

Engaging in any activity which is illegal under any applicable law. Such violations may constitute a criminal offense. You are prohibited from accessing websites, web-directories or similar sources hosting or containing unlawful, immoral, or criminal material, material which is liable to cause embarrassment to others, or otherwise inappropriate content (such as online gambling sites or sites containing pornographic material). The Company recognizes that it is possible to inadvertently access such sites, and you will have the opportunity to explain any accidental breaches of this Policy.

D. Improper Disclosure of Confidential Information

Disclosing or sharing Restricted, Highly Confidential and Confidential information with third parties unless such disclosure is permitted or authorized by law and a Non-Disclosure Agreement (NDA), Data Processing Agreement or other suitable agreement has been signed by authorized Company Personnel. The disclosure must also be deemed appropriate given the volume and sensitivity of the information.

E. Legal or Other Harm to Company or Others
Causing legal liability for the Company or damage the Company's brand or reputation or causing damage, distress, or any other form of harm to others.

F. Disruption/Damage or Unauthorized Access
Doing anything to disrupt, damage, impair, interrupt, slow down, interfere with or affect the functionality of the Electronic Resources, including any computer hardware or software, beyond your normal use. You must not attempt to gain access to restricted areas of the Company's network, systems, databases or to any other password-protected information, unless you are specifically authorized. For the purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. You must not grant any access to the network, systems, databases or to any other password-protection information of the Company to any person who has not been duly authorized by the Company. If you are in any doubt, you must obtain written permission to the standard set out in paragraph 7 below.

G. Viruses
Knowingly uploading, transmitting or posting any material that contains viruses, worms, time-bombs, keystroke loggers, spyware, adware, Trojan Horses or any other harmful files, programs or other similar computer code designed to adversely affect the operation of any computer software or hardware.

H. Social Networks/Website- Violation of Terms of Use
Using social networks or other websites in violation of their posted terms and conditions.

I. Advertisement or Inappropriate Solicitation
Advertise or offer to sell or buy any goods and services for any business purpose, unless specifically permitted to do so by your manager. Make or circulate commercial, religious or political statements or solicitations, or promote businesses unrelated to the Company.

J. Impersonation
Impersonating another person or entity or create a false identity for the purpose of misleading another person.

K. Sending Email Without Consent or an Unsubscribe Mechanism, Where Required
Sending unsolicited email to any individual, business, or entity with whom you do not have an established business relationship or documented prior express or implied consent where such consent is required under applicable data protection law or sending email that does not have a working unsubscribe mechanism where one is required (for example, as needed to comply with CAN-SPAM, CASL, the e-Privacy Directive). If you are unsure if you need consent or an unsubscribe mechanism, please contact the Global Privacy Office.

L. Copyright Violation
Downloading, copying and/or distributing copyrighted material including, but not limited to, digitizing and distributing music, movies, games, text or photographs from magazines, books, websites or other copyrighted sources, without prior authorization by the content owner.

M. Install Unauthorized Software
Downloading or installing any software onto Electronic Resources that hasn't already received prior approval by the Company without obtaining prior authorization from the Information Security Office.

N. Fraud/Misleading Statements or Fraudulent Email Headers

Making fraudulent, misleading offers of products, items, or services. Any offers made for or on behalf of the Company must be authorized by your manager or supervisor. Engaging in unauthorized use or forging of email header information.

O. Unauthorized Company Warranties/Guarantees/Representations/Contractual Commitments

Making statements about warranties or guarantees (expressly or implied) regarding the Company unless it is a part of your normal job duties and has been agreed to by your manager. Agreeing to terms, entering into contractual commitments or making representations by email unless appropriate authority has been obtained.

P. Unapproved Wired Device Connections

Connecting any device that is not a Company approved Electronic Resource (for example a personal laptop) to the Company's wired network without approval from the Information Security Office.

Q. Unsecured Wireless Connections

Conducting business activities, connecting to your email or transmitting Company information across any wireless network connection that is not properly secured according to the standards of the Information Security Office. For example, using the Company provided virtual private network (e.g., Global Connect) is considered secured and meets the standards.

R. Inappropriate Sharing of Electronic Resources

Sharing Electronic Resources with family, friends and other third parties.

S. Sending Trivial/Unnecessary Emails

Contributing to system congestion by sending, uploading, posting or forwarding unauthorized or unsolicited advertising, promotional materials, “junk mail”, “spam”, “chain letters”, “pyramid schemes” or any duplicative or unsolicited trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them.

T. Improper Use of Another Person’s Computer or Email/Assumed Identity

Sending messages from another Company Personnel’s computer or email account or under an assumed name unless specifically authorized by the Information Security Office.

U. Unsecure Sending, Storing or Providing Access to Sensitive Personal Data

Using the Company's systems to send Sensitive Personal Data via email, the Internet, instant messaging or by other means of external communication which are not known to be secure. Storing Sensitive Personal Data locally on Electronic Resources or in file shares that are not secure or providing inappropriate access to the Sensitive Personal Data.

5.3 USE OF ELECTRONIC MAIL (EMAIL) - PRECAUTIONS

A. Draft Carefully – Messages Can Be Forwarded

You should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality, breach of contract or cause any other harm. As emails can be easily forwarded to multiple recipients, you should assume that email messages may be read by persons other than the intended recipients.

B. Legal Production of Emails

Email messages may be disclosed in legal proceedings and provided to individuals in response to a subject access request under applicable data protection legislation, in the same way as paper documents and other records. Even though you delete an email from your inbox or archives, that does not mean that an email cannot be recovered for the purposes of disclosure. You should treat all email messages as potentially retrievable, either from the main server or using specialized software, in accordance with Company policies and applicable laws.

C. Phishing - Emails from Unknown Sources

Phishing is the most common way for bad actors to try to compromise Company systems. You should never reply to, act on, forward, click on links or open attachments (especially any file that ends in .exe) related to emails that you believe to be a phishing attempt or when you are unsure of the source of the sender of the email. If you suspect that you have acted on such an email, you should report it immediately as an incident. If you receive an email you believe to be a phishing attempt, you should use the Company's phishing incident reporting application in Outlook or if you do not have the phishing application, then report it as an incident by following the steps outlined in Section 2.

D. Shared Email Inboxes

Shared mailboxes must be approved by the Information Security Office and have an individual assigned as the owner who is responsible for all activity involving that mailbox.

E. Receipt of Wrongly Delivered Email

If you receive a wrongly-delivered email, you must notify the sender, but you must not respond to SPAM or phishing emails.

F. Use of Email Forwarding Rules

The use of email forwarding rules set-up to forward the receipt of Company emails to non-Company email addresses is prohibited without a valid business justification which must be approved by the Information Security Office.

5.4 Use of External or Cloud Services

A. Approved External Cloud or External Hosting Services

The Information Security Office will maintain a list of approved external vendors providing cloud or external hosted Electronic Resource services to the Company, for example Salesforce.com. You may only use cloud services on the approved list. The Information Security Office will audit the approved vendors on a regular basis for compliance with the Company's security and privacy requirements and will assign each vendor a qualified level of information classification for the service.

B. Reporting Incidents Regarding Cloud Services

You must report as an incident the transmission or storage of Company information with an unapproved cloud service or the transmission or storage of Company information above the qualified level of the vendor.

5.5 Use of Electronic Resources for Payment Card (Credit Card) Transactions

If you accept payments through a payment card (any type of credit card) on behalf of the Company using Electronic Resources, you must only use Electronic Resources that have been audited and approved by the Information Security Office for compliance with the current Payment Card Industry Data Security Standard.

5.6 USE OF THUMB DRIVES AND EXTERNAL STORAGE MEDIA

You must not transfer Company information (in any format) to external storage media or portable devices or equipment (fixed/external hard disk, USB/Memory-Stick, CDs/DVDs, etc.) not provided and, where appropriate, configured by the Company. Any such device or equipment containing Sensitive Personal Data or any other data that qualifies as Restricted under the Company's Information Classification Policy must be encrypted using a solution approved by the Information Security Office and in compliance with the Information Security Policy.

5.7 SECURITY, ACCOUNTS AND PASSWORDS FOR ELECTRONIC RESOURCES

A. Information Security Policy

You are responsible for protecting Electronic Resources as required by the Company's Information Security Policy.

B. Creating and Changing Passwords

You must create a unique password for your accounts and not re-use passwords for the same account according to the rules for that account regarding prior passwords. You must change your account password on the schedule required by the Company. You must ensure the confidentiality of your account password by not revealing it to or sharing it with others or allowing others to use your account. This includes family and other household members when work is being done at home.

C. Communicating Passwords

If you communicate passwords or other secret authentication information, you must do so securely according to the standards of the Information Security Office. For example, if you need to provide a password, do not include it in an email sent with the file that is password protected. It is a best practice to call the receiver of the file and provide the password by phone or otherwise provide it in a way that won't compromise the file if the inbox receiving the file or the transmission of any emails is not secure.

D. Privileged Access Accounts

The Information Security Office will tightly control privileged access accounts (admin accounts, root accounts, etc.) and such accounts must only be created and/or issued with the approval of the Information Security Office. Privileged access accounts and their use must comply with all standards and procedures issued by the Information Security Office.

5.8 USE OF ELECTRONIC RESOURCES FOR TELECOMMUTING/REMOTE WORK

A. Working at Client Sites

As noted in the Scope section of this Policy, if you are operating at a third party site that is not controlled by the Company (for example a Company client site or remotely but for the benefit of a client) and/or using client issued Electronic Resources, in addition to the policies provided to you by the Company, you may be subject to additional policies provided to you by that third party, and you agree to comply with those policies. Unless otherwise directed by a client, you agree:

- Not to store locally on the Electronic Resources or transmit to any external device any client confidential or proprietary information or any Sensitive Personal Data, regardless of whether the Sensitive Personal Data originates from the client or some other source;
- To follow the "stand up, lock up" practice of locking the Electronic Resources when stepping away, no matter how briefly as required by the Company's Information Security Policy;
- To utilize any VPN or other specific protocol for accessing the client's network; and

- To not use any personal devices or personal equipment.

B. Working at Home or other Remote Worksites

If you are operating at a home office, airport, hotel or other remote site not controlled by the Company, then you are responsible for following this Policy and the Information Security Policy in those remote work environments. In Company locations where implemented, the use of multi-factor authentication (MFA) to the GlobalProtect VPN is required for remote logins when connecting your Company-issued computer or laptop to Company network services.

C. Conflicts in Policies

In the event there is a conflict between any policies you have received from the Company and any policies you receive from a client or other third party, you should follow the Policy that best ensures the rigorous protection and safekeeping of any Electronic Resources you are using, as well as the data contained within them. If you are not sure what you should do, you must reach out to your direct supervisor at the Company and to an appropriate contact at the client or other third party for guidance.

5.9 MONITORING OF ELECTRONIC RESOURCES

For information regarding how the Company monitors your use of Electronic Resources, see the Company's Workplace Monitoring Policy.

5.10 RETURN OF ELECTRONIC RESOURCES FROM DEPARTING EMPLOYEES/CONTRACTORS

You must return all Electronic Resources that belong to the Company or to a client upon any separation of your employment or engagement with the Company (for example, laptops, mobile phones, iPads/tablets, thumb drives/storage devices, key fobs/access badges). You must return the Electronic Resources in the same condition as when it was delivered to you, absent any normal wear and tear. Upon your separation, the Company will disconnect you from all Electronic Resources, including, without limitation access to the Company's email and the Company's networks, intranet, applications (for example, Salesforce.com) or other Company-paid subscription services (for example, LinkedIn Premium or research tools) and network and file shares (for example Microsoft Teams sites and network file shares such as O:, Q:, S:, T:, and U:.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company- provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 EXCEPTION HANDLING

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

9 DOCUMENT INFORMATION

Document Name	Acceptable Use of Electronic Resources Policy
Issue Date	January 1, 2025
Next Review Date	January 1, 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Craig White
Owner	Andy Sheppard

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Nov. 1, 2011	First version under name “Electronic Resources Policy”
2.0	Nov. 1, 2012	Annual review
3.0	Jan. 1, 2013	Annual Review; changed to 1/1 review cycle
4.0	Jan. 1, 2014	Annual Review
5.0	Jan. 1, 2015	Annual Review
6.0	June 1, 2016	Name of Policy changed to “Acceptable Use Policy”
7.0	Jan. 1, 2017	Annual Review – updated definition of Electronic Resources and Sensitive Personal Data; added training and education to enforcement section; minor typos and wording changes
8.0	Nov. 18, 2018	Annual review – no changes made
9.0	Jan. 1, 2020	used new template; changed name of Policy to “Acceptable Use of Electronic Resources Policy; updated Policy for GDPR; revised organization to make it easier to digest for reader
10.0	Jan 1, 2021	Annual review – added examples for clarity; minor wording changes and typos
11.0	Jan 1, 2022	Annual review – added e-mail forwarding rules; updated definition of Sensitive Personal Data to match change made in other policies; minor wording changes and typos
12.0	Jan 1, 2023	Annual review – updated definitions for Social Media and Sensitive Personal Data to match changes made to those definitions in the Social Media Policy and Personal Data Protection Policy, respectively; minor typos and wording changes
13.0	Jan 1, 2024	Annual review - added clarification of information security incident to incident reporting section; added clarification that MFA for VPN may

		be required for remote access; added full ist of Information Security Framework policies; minor wording changes.
14.0	Jan 1, 2025	Annual review – Changes to Incident Reporting and scope section consistent with changes made in all Information Security Program policies; added defined term of “Europe” for the EEA, UK and Switzerland and made appropriate changes throughout; updated Social Media definition for changes in names of platforms; other minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Bring Your Own Device ("BYOD") Policy

Document ID:	AG-ISMS-POL-BYO
Version Number:	8.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Bring Your Own Device ("BYOD") Policy (the "Policy") is part of the Information Security Policies Framework and explains how you are able to connect your personal mobile phone devices and tablets (such as iPads) (collectively "Personal Device") to the Company's network or other resources and the remote access that the Company will have to the Personal Device (the "BYOD Program"). You are not permitted to connect a personal laptop or computer to the Company's network. . This Policy reflects the state of technology as of the date of its adoption; therefore, technological developments may exceed the literal text of this Policy.

The BYOD Program is entirely voluntary unless otherwise stated in a separate policy that has been provided to you and/or if you are not reimbursed by the Company for your Personal Device (see Par. 5.1) You may choose not to participate in the BYOD Program for any reason without explanation.

For security reasons, you are not permitted to connect your Personal Device to the Company's telecommunications and IS networks unless you participate in the BYOD Program. However, you may (i) access webmail via a browser, (ii) access our guest Wi-Fi network and adhere to the guest network Wi-Fi terms and conditions, (iii) receive a multi-factor (MFA) communication (e.g. text or phone call) or (iv) receive texts and calls as a general means for the Company to contact you on a Personal Device without participating in the BYOD Program. For the avoidance of doubt, this Policy and the BYOD Program do not apply to any of the foregoing uses of your Personal Device.

Please see the Company's Workforce Monitoring Policy for additional information that may apply to these uses of your Personal Device.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them.

The Company needs your help in identifying those incidents and violations. An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section shall, for all purposes of this Policy, have the meanings specified as follows:

(1) "**BYOD**" means Bring Your Own Device

(2) "**BYOD Program**" means the Company program for you to connect your Personal Devices to the Company's network or other resources and the remote access the Company will have to the Personal Devices to allow that connection.
(3) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We" or "us" or "Us".
(4) "**Company Data**" means all data contained in the Company provided applications set forth in Paragraph 5.3E and all data contained in any emails directed to or from a Company-issued email address.
(5) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".
(6) "**Information Security Program Framework"** means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.
(7) "**MDM Application**" means the application the Company uses for mobile device management of your Personal Device as part of the BYOD Program. It allows the company to separate work applications from your personal applications on your Personal Device.
(8) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).
(9) "**Personal Device**" means collectively your personal mobile phone or tablet (such as an iPad).

4 SCOPE

The target audience of this policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote location). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own policy, as long as such policy is no less rigorous than this Policy.

This policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems equipment.

This policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 How to Participate in the BYOD Program

A. Download MDM Application and Consent to Policy to Participate

If you wish to participate in the BYOD Program, you must download the MDM Application to your Personal Device. As part of the process of downloading the MDM Application, you must consent to adherence to this Policy by accepting the terms and conditions provided by the Company during the initialization of the MDM Application. Your continued participation in the BYOD Program will be considered ongoing consent to this Policy.

B. Personal Device Reimbursement

If you receive a stipend for your Personal Device, you are expected to participate in the BYOD Program and agree to the terms and conditions.

5.2 MDM Application in BYOD Program

A. Description of MDM Application

The Company uses a third-party MDM Application which provides the Company the ability to identify Company data and to separate it from the non-Company Data on your Personal Device.

B. MDM Application Requirements

The MDM Application will require you to:

- Accept the MDM Application terms and conditions;
- Enter a secure password and/or PIN that meets the Company's password standards prior to you accessing any Company data on your Personal Device; and
- Require your Personal Device to automatically lock after it is idle for five (5) minutes.

5.3 Your Responsibilities and Personal Device Security Requirements During BYOD Program

A. Update Personal Device Operating System

You must keep your Personal Device's operating system updated. The Company will support the latest two supported full versions of operating systems per Personal Device type (iOS, Android, Windows). The Company will terminate your participation in the BYOD Program (see Sec. 5.6) if you do not keep your Personal Device operating system updated to what the Company will support.

B. Maintain Relationship with Wireless Carrier

You are responsible for any Personal Device registration with the vendor and/or service provider, maintaining any necessary warranty information, settling any service or billing disputes with the wireless carrier and purchasing any required software or Personal Device related accessories. The Company will provide, pay for and manage the MDM Application.

C. Battery Replacement/Power Source

You are responsible for providing sufficient battery power for the Personal Device to maintain power. If your Personal Device is without power for 30 days, the Company will terminate your participation in the BYOD Program (see Sec. 5.6).

D. Back-up of Personal Data

You are responsible for the back-up of any data on your Personal Device other than the Company data.

E. Use of Company Provided Applications

A number of applications are made available for use within the BYOD Program as these applications can assist you in working remotely (for example, Microsoft Outlook, Microsoft Teams, Viva Engage, Word and Excel). The Outlook application is required. More information on these applications is available on the Company's intranet. Only approved, corporate applications may be used for work purposes (for example the Outlook application for email)..

F. Email Must Be Used Through Work Email Address and Outlook Application

You are permitted to use your Personal Device for work-related correspondence, including email between Company Personnel, clients, suppliers and other individuals or organizations. This may only be done through your Company-issued email address, which means you must use the Outlook application tied to the MDM Application and not the email application available on your Personal Device (for example, on an iPhone the envelope icon). You must not use personal email addresses (for example, a Gmail or Yahoo email address) to send or receive work-related correspondence or documentation.

G. Virus Protection for Personal Devices

The Company may require you to use, apply or update anti-virus/malware protection for any Personal Device in the BYOD Program. If you receive such a request, you must comply with it.

H. Compliance with Acceptable Use of Electronic Resources Policy

Your use of your Personal Device as it relates to the Company is subject to compliance with the Company's Acceptable Use of Electronic Resources Policy.

I. Technological Support

The Company does not provide technological support for Personal Devices outside of assistance with the MDM application (enrollment, configuration, etc.). You acknowledge that you alone are responsible for any repairs, maintenance or replacement costs and services.

J. Confidential and Proprietary Rights

The Company's confidential information and intellectual property, including trade secrets, are extremely valuable to the Company. You must treat them accordingly and not jeopardize them through your use of your Personal Device. Disclosure of the Company's confidential information to anyone outside the company and use of the Company's intellectual property is subject to this Policy and all other applicable Information Security Framework Policies as well as the Employee Handbook and the Company's Code of Conduct.

5.4 How the Company Handles Personal Data in the BYOD Program

A. Personal Data Collected at Initial Participation

At the sign-up stage, certain information (see 5.4 B below) will be automatically collected in order to participate in the BYOD Program. The Personal Data that is being processed is limited only to that which is necessary to carry out the services provided and to ensure compliance with the BYOD Program. If you do not consent to this this information being collected, you will not be able to participate in the BYOD Program.

B. MDM Application Collection of Personal Data

The MDM Application will collect and store information related to participation of the Personal Device in the BYOD Program, including the following information from your Personal Device:

- Normal home country of the Personal Device;
- Personal Device operating system and version;
- Personal Device make and model;
- Personal Device unique identifying number;

- Time of the last contact between the Personal Device and the MDM Application; and
- Time the Personal Device was registered to the BYOD Program.

C. Minimization of Personal Data Collection

The Company will not use the MDM Application or participation process to collect or process Personal Data for any purpose other than the management of the BYOD Program or in any way that is not proportionate to the legitimate objectives of the BYOD Program.

D. Security of Personal Data Collected

The Company will implement appropriate technical and organizational measures with regards to the Personal Data collected for the purposes of the BYOD Program and will handle the Personal Data in accordance with the Company's Personal Data Protection Policy.

5.5 MONITORING IN THE BYOD PROGRAM

A. No Expectation of Privacy

All material, data, communications, and information created on, received, or transmitted by, printed from, or stored or recorded on any of the Company applications described in Paragraph 5.3E is the property of the Company, regardless of who owns the device(s) used. You are expressly advised that in order to prevent misuse, the company reserves the right to monitor, intercept, review, and remotely wipe, without further notice, all Company data in the Company's sole discretion. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings, and other uses of the device, whether the device is in your possession or the Company's possession. **Therefore, you should have no expectation of privacy whatsoever in any Company Data.** The Company may also make and preserve copies of all Company Data, including Personal Data, in its sole discretion, for a period of time after those copies are created and may delete those copies from time to time without notice. In addition, the Company may obtain and disclose copies of any Company Data for litigation, investigations, and as otherwise required by law.

B. MDM Application Does Not Monitor Content Unless It Is Company Data

The MDM Application does not permit monitoring of, and therefore the Company will NOT monitor, the content of any communications to or from Personal Devices that are not directed to or from a Company-issued email address, applications installed as part of the MDM Application or other Company telecommunications facility accessible via the Personal Device.

C. No Monitoring of Application Data on Personal Devices

The Company does not currently monitor application data on Personal Devices unless it is application data that is Company Data; however, the Company may, in the future, be notified of certain applications that could pose a security threat to its network. If the Company is notified of applications that may pose a threat, you will be notified, and such applications will be placed on a blacklist. If a blacklisted application exists on your Personal Device or is subsequently downloaded, the Company will be alerted by the MDM Software and will immediately disconnect your Device from the BYOD Program and remove any Company data from the Device until the application is removed.

D. Monitoring of Company Emails and Texts

Any Company emails (including attachments) and Company related texts on your Personal Device may be monitored as further explained in the Company's Workplace Monitoring Policy and as set forth in Paragraph 5.5A.

5.6 How You Can Withdraw from and What Terminates You From the BYOD Program

Once you have joined the BYOD Program, the following explains how you can withdraw from or be terminated from the BYOD Program:

A. Withdraw - You Delete the MDM Application from Your Personal Device

You can delete the MDM Application from your Personal Device to withdraw your consent to this Policy and withdraw your participation.

B. Terminate - MDM Alerts – Failure to Comply with BYOD Program Requirements

(1) Personal Device Off For 30 Days

The Company will be alerted if a Personal Device has not been turned on for 30 days.

(2) Failure to Update Operating System

The Company will support the latest two supported full versions of operating systems per Personal Device type (iOS, Android, Windows). If your Personal Device's operating system falls below this acceptable standard, the Company will be alerted.

(3) Jailbreaking and Rooting

The MDM Application will inform the Company if the MDM Application on a Personal Device has been modified to allow root access to the Personal Device's operating system, unauthorized elevation of user privileges or circumvention of the Personal Device's security measures. This is sometimes referred to as "jailbreaking" for Personal Devices running Apple iOS, and "rooting" for Personal Devices running the Android operating system.

(4) Use of Blacklisted Application

As noted in Paragraph 5.5C, if your Personal Device has a blacklisted application on it, the Company will be alerted by the MDM Software.

(5) Failure to Use Anti-Virus When Requested

If the Company requests that you use, apply or update anti-virus/malware protection for your Personal Device, you must comply with the request to stay in the BYOD Program.

(6) Failure to Comply with the Electronic Resources Policy

If you use your Personal Device in a way that violates the Acceptable Use of Electronic Resources Policy, the Company may terminate your participation in the BYOD Program.

C. Terminate - Lost/Stolen Personal Device

If your Personal Device is lost, stolen or otherwise unaccounted for, you must immediately report it to the Company as an incident as described in Section 2. If it was stolen you are advised to report it to the police; however, since it is a Personal Device, whether or not to report it to the police is at your discretion.

D. Terminate - Ceasing Use of Personal Device

In the event that you change or stop using a Personal Device which has the MDM Application installed, you must un-enroll that device by deleting the MDM Application (or by restoring the

Personal Device to its original factory settings which will remove the MDM Application). You should contact the IS service desk if you need help with un-enrolling your device.

E. Terminate - Separation from Employment or Engagement/Leave of Absence

If you separate from employment or engagement with the Company, the Company will terminate your Personal Device from the BYOD Program. In addition, the Company may elect to terminate your Personal Device from the BYOD Program if you will be on a leave of absence likely to last more than three weeks; however, the Company would discuss this with you prior to taking any action.

F. Consequences of Withdrawal or Termination from BYOD Program

For security reasons, if you withdraw from the BYOD Program or you are terminated from the BYOD Program for any of the reasons in this Section 5.6, the Company will disconnect your Personal Device from the BYOD Program and erase all Company data from your Personal Device. Your Personal Device will not be allowed to reconnect to the BYOD Program until it is in compliance with this Policy, including all the provisions in this Section 5.6.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 EXCEPTION HANDLING

While every exception to a policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Acceptable Use of Electronic Resources Policy
- Information Security Policy
- Personal Data Protection Policy
- Workplace Monitoring Policy

9 DOCUMENT INFORMATION

Document Name	Bring Your Own Device (“BYOD”) Policy
Issue Date	January 1, 2025

Next Review Date	January 1, 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Craig White
Owner	Andrew Sheppard

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	March 1, 2017	First version
2.0	Nov. 18, 2018	Annual Review – revised logo
3.0	Jan. 1, 2020	Annual Review –used new template; organized content to make it more readable for the user
4.0	Jan. 1, 2021	Annual review – minor wording changes and typos
5.0	Jan 1, 2022	Annual review – provided clarifying explanation that laptops are subject to the Acceptable Use of Electronic Resources Policy and not this BYOD Program; added clarifying explanation that monitoring of Company emails is still subject to the Workplace Monitoring Policy; minor wording changes and typos
6.0	Jan 1, 2023	Annual review – clarified that MDM will not require that you change your password periodically; noted that the Personal Data collected is kept to the minimum necessary; added that you can dis-enroll a device by deleting the MDM application or restoring to factory settings
7.0	Jan 1, 2024	Annual review - added clarification of information security incident to incident reporting section; added clarification that this Policy does not apply to use of Personal Device for MFA purposes; added full ist of Information Security Framework policies
8.0	Jan 1, 2025	Annual review – Updates to Incident Response and Scope sections consistent with changes made to all Information Security Framework policies; clarified definition of information assets and Personal Data to be defined collectively as “Protected Assets”; clarified application of this Policy to laptops and other devices besides mobile phones; added definition for “Company Data” and clarified how MDM separates Company Data from non-Company Data; added new Paragraphs to Section 5.3 regarding technological support, costs and reimbursements and confidential and proprietary rights; added a “No Expectation of Privacy” Section 5.5.A to clarify the monitoring that occurs in addition to citing to the Workplace Monitoring Policy; [clarified reporting obligations for a lost Personal Device; other minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Information Security Policy

Document ID:	AG-ISMS-POL-ISP
Version Number:	14.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Information Security Policy (the "Policy") is part of the Information Security Policies Framework and contains important rules covering information security and protecting the confidentiality, integrity, and availability of Personal Data and information assets (collectively "Protected Assets") within the Company. This Policy establishes safeguards and controls to protect the Company's Protected Assets from loss and from unauthorized access, modification, destruction, or disclosure.

Senior leadership of the Company is committed to satisfying applicable requirements related to information security and to continuous improvement of the information security management system.

This Policy will be reviewed on an annual basis or upon any changes that have a direct and material impact on the Policy controls and objectives.

The Company's information security objectives include:

- Implementing proactive measures to protect the confidentiality, integrity and availability of Protected Assets;
- Improving the efficiency and effectiveness of information security operations and functions; and
- Minimizing the risk of unauthorized disclosure and access to confidential assets.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(2) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's

Protected Assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(3) "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

(4) "**Electronic Resources**" means any (a) information technology equipment, devices or related equipment (such as servers, computers, laptops, desk phones, mobile phones, tablet PCs (e.g., iPad), thumb drives or other storage devices or multi-function printer/copier/scanner/fax machines); (b) electronic key fobs/cards; (c) internet and internet connections; (d) intranets; (e) network file shares (such as the Q:, S:, T:, U: or O: drives); (f) file sharing sites (such as Team Sites, OneDrive and SharePoint); (g) databases; (h) online subscriptions and services (such as WebEx or LinkedIn Recruiter); (i) applications, whether cloud or on-premise (such as Office 365, voice mail, PeopleSoft, Salesforce ("Connected") or Bullhorn); (j) wearable or 'nearable' devices or any equipment comprising the 'internet of things' and (k) CCTV and any other similar resources of any kind each of which are (i) supplied by the Company to you for use for work-related purposes or (ii) not supplied by the Company to you, but are either: (a) used by you to connect to any Company network or (b) used in a way that relates to the Company and/or your work on behalf of the Company, whether intended or not.

(5) "**European Sensitive Personal Data**" means information collected from or about individuals in Europe (collectively "Europe" for purposes of this Policy refers to the EEA countries, the UK, and Switzerland) relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, as well as data concerning health or data concerning a person's sex life or sexual orientation. In some European member states, it may also include information about a person's criminal convictions.

(6) "**Information Security Policies Framework"** means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(7) **"ISO"** means International Organization for Standardization that issues the ISO/IEC 27000 series of standards to help companies keep Protected Assets secure.

(8) **"NIST"** means the National Institute of Standards and Technology, a U.S. organization that issues an information security framework of standards to help companies keep Protected Assets secure.

(9) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(10) "**Sensitive Personal Data**" means collectively European Sensitive Personal Data, any type of Personal Data that is considered "sensitive" data under applicable data protection law and for all individuals, regardless of applicable data protection law, includes health data, biometric data, genetic data, certain financial data, specifically, an individual's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, immigration and citizenship status and social security numbers or other national identification numbers and national identity documentation (such as passports).

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote location). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own policy, as long as such policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 INFORMATION SECURITY GOVERNANCE

A. Senior Leadership Commitment to Security and Privacy

The Company's senior leadership is committed to establishing and promoting a secure organization that values security and privacy and provides financial support and executive oversight of security and privacy initiatives. The Company maintains a Data Protection Oversight Committee that includes senior executives of Allegis Group to provide appropriate oversight related to privacy and security issues

B. Information Security Office – Organization

The Information Security Office is responsible for authorizing, supporting and executing on the Information Security Policies Framework. The Information Security Office regularly reviews risks to balance security controls with business needs. The Information Security Office has appointed an Executive Director to head the Information Security Office. A member of the Information Security Office is dedicated to managing governance and compliance for the policies within the Information Security Policies Framework, with responsibility for auditing compliance with the policies and the underlying standards and processes of the Information Security Policies Framework, including aligning such standards to recognized standards issued by organizations such as NIST and ISO. The Information Security Office includes a role dedicated to security by design. The Information Security Office will ensure that its Company Personnel have the required competencies, by means of suitable education, training and certifications, or experience, to execute their roles.

C. Global Privacy Office – Organization

The Global Privacy Office is part of the Legal Department. The Global Privacy Office has appointed a Vice President to head the Global Privacy Office. The Company Personnel in the Global Privacy Office work closely with the Information Security Office in drafting and reviewing the Information Security Policies Framework, in particular with regards to any policies that address privacy issues. The Global Privacy Office will ensure that its Company Personnel have the required competencies, by means of suitable education, training and

certifications, or experience, to execute their roles, including without limitation obtaining privacy certifications through the International Association of Privacy Professionals.

D. Privacy and Protection Team – IS - Organization

The Privacy and Protection Team ("PPT") is part of the Data Governance team within the IS Department. The PPT, Data Governance and Master Data Management Teams within IS are all under the combined leadership of an IS Delivery Manager, Executive Director and Vice President within the IS Department. The Privacy and Protection Team includes roles focused on records management issues and data minimization. The Global Privacy Office will ensure that its Company Personnel have the required competencies, by means of suitable education, training and certifications, or experience, to execute their roles.

E. AI Center of Excellence – IS – Organization

The AI Center of Excellence is a part of the IS Organization and reports to the Sr. VP of Digital Transformation. The AI Center of Excellence has dedicated Company Personnel who are responsible for developing, implementing and maintaining an AI Governance program. The AI Center of Excellence works closely with the Information Security team, the Global Privacy Office and the Third Party Risk Management Team. The AI Center of Excellence will ensure that its Company Personnel have the required competencies, by means of suitable education, training and certifications, or experience, to execute their roles.

5.2 ELECTRONIC RESOURCES USE

A. Acceptable Use of Electronic Resources Policy

You must follow the Company's Acceptable Use of Electronic Resources Policy, which details your obligations regarding the use of things like laptops, thumb drives, mobile phones and tablets. The Information Security Office will be responsible for logging and tracking all devices that are Electronic Resources, for example laptops, according to standards set by the Information Security Office.

B. Assignment of User Accounts

Your access to Company systems must be authorized through the assignment of an individual user account by the IS Department.

C. IS Department Responsibilities

If you are a part of the Company's IS Department, you will take measures to protect data, including following security acceptance testing programs, change management programs, encryption requirements, authorization requirements, backups, and other procedures to the standards set by the Information Security Office.

5.3 INFORMATION CLASSIFICATION AND HANDLING

You are responsible for labelling information and handling information according to the Company's Information Classification Policy. The Information Security Office is responsible for issuing standards for specific functions within the Company, for example the Information Security Office and IS, to support the Information Classification Policy. The following is additional guidance regarding data handling:

A. Use of Designated Systems

The Company expects all Company Personnel to only process Personal Data using systems approved by the Company for the processing activity. Department heads must ensure their teams have suitable systems for the processing activities they perform and guidance on how to correctly use those systems. They should raise any concerns by reporting such concerns as an

incident under this Policy. As much as possible, Company Personnel should avoid using their own manual or 'offline' methods such as, and without limitation:

- Using their own spreadsheets or other documents to keep lists of contacts, candidates or other Data Subjects instead of using the appropriate Company system;
- Saving Company records on desktops or in personal folders rather than in the designated Company system for those records;
- Saving copies of emails outside their mailboxes or other Company approved locations such as document management systems;
- Printing, copying, emailing or extracting material from a Company system, except for limited short-term use (for example for reference or ease of reading) and then destroying such information when the short-term use has ended (see Disposal of Manual Records below); or
- Unnecessarily emailing colleagues documents which are accessible on the designated company system.

B. Disposal of Manual Records

Although it should be kept to a minimum, the Company recognizes that use of personal files, notes, working documents, print-outs, and/or hard copies ("Manual Records") may be necessary for teams or individual members of Company Personnel to achieve their objectives and perform their work. Where Company Personnel have created Manual Records containing Personal Data, they must be disposed of as soon as possible when they are no longer needed. For example:

- Paper notes about a meeting or phone call should be destroyed once the relevant facts are recorded in the appropriate Company system;
- A spreadsheet used to decide which candidates to shortlist to a client for a vacancy should be disposed of once the shortlist is sent; and
- Print-outs must be disposed of once members of Company Personnel have finished using them.

For the purpose of this section, 'disposing of' a record means:

- For computer files, permanently deleting (e.g. emptying the "recycle bin" on Windows PCs) all copies from all file locations (including your desktop, personal drive, any portable media, and any shared drives); and
- For paper records, disposing of the record as confidential waste according to the procedures in place in the location (which, in most locations will entail shredding the document, or placing the document in the secure waste bins provided).

C. Password Protection of Email Attachments

Accidently emailing Personal Data to the wrong recipients or accidently emailing more Personal Data than was intended form the most frequent causes of Personal Data breaches. For this reason, relevant documents should be password protected (so that the document cannot be opened without the password) before they are sent as email attachments if unintended disclosure of the document's contents presents any significant risk to any Data Subjects identified in that document. The Company takes a risk-based approach and does not require all email attachments containing Personal Data to be encrypted or password protected as this would be disproportionate and would significantly impact the effectiveness of our services and the likelihood of consistent data protection compliance. Passwords should be used when the document:

- **Significant Volume of Personal Data –** contains Personal Data on a significant number of Data Subjects (even if that data is not particularly sensitive or confidential);
- **Significant Confidential Nature of Sensitive Personal Data –** contains Personal Data which is significantly confidential or sensitive (even if that data only identifies a relatively small number of Data Subjects); or

- **Distribution to Large Number of Recipients –** contains Personal Data and will be distributed to a large number of people or otherwise used in a way that makes it more likely to be accidently disclosed.

Examples of documents that would require password protection are:

- Reports/spreadsheets containing information about a number of people (such as a list of all current contractors at a particular client);
- Status reports with detailed information on the performance or conduct of one or more people; and/or
- Copies of passports, medical reports or other sensitive documents.

Although care must always be taken to only send to the correct recipients, password protection is not required when sending:

- A CV (or small number of CVs) to a client contact;
- Invoices and timesheets; and/or
- Any document that is publicly available (e.g. material posted on our external website)

More specific guidance on particular documents and situations may be issued by department leaders. Please note these examples focus on a requirement to password protect for data protection reasons. Documents may also need to be password protected for other reasons, such as confidentiality, even if they do not contain any Personal Data. In addition, you are encouraged to consider methods other than email for transmitting documents that need to be password-protected such asloading them to an encrypted thumb drive to mail to the recipient (and then call the recipient to provide the password) or upload them to a secure FTP site where available (for example when sending files to a vendor, they may provide such an FTP portal). You should reference the Information Classification Policy for more information regarding categories of data and how to handle them.

D. Effective Password Protection

For Microsoft Office documents, the option to add password protection can be found on the application's main menu under File/Info/Protect Document>Encrypt with Password.
When sending emails with a password protected document(s):

- Use a password that is not obvious;
- Do not use the same password every time;
- Do not include the password in the same email as the document; and
- Where practical, communicate the password by a means other than email (to reduce the risk of sending both the password and the document to the same incorrect email address).

E. Other Electronic Communications

The rules in this section concerning email also apply equally to all methods of electronic communication.

5.4 PHYSICAL SECURITY

A. Access to the Organization's Premises

Access to any Company premises is for authorized Company Personnel only through the allocation of either an identity card or visitor's pass. Any person authorized via a visitor's pass must be accompanied by Company Personnel when moving around the office apart from in client areas such as client meeting room facilities. You must carry your Company-issued ID and/or other required identity at all times while on the premises and present them upon request. Access to the building is recorded for security purposes through CCTV and access management systems. The Information Security Office is responsible for issuing any standards related to physical security access.

B. Secure Areas and Secure Area Access

Within Company premises, there are secure areas where access is limited to specifically authorized Company Personnel for security or health and safety reasons. Authorization must be approved for areas such as server rooms, secure meeting rooms, power rooms, and project areas. These areas are labelled as such and guidance is available from the Information Security Office on how to obtain authorization for these areas. You may not attempt to gain access to these areas without authorization, even when you are accompanied by an authorized person. All access to secured areas must be logged and all logs must be reviewed at least monthly. Procedures for working in secure areas will be documented and enforced at all times. All those with access to the secure areas will be trained in these procedures.

C. Control over Electronic Resources – "Stand Up, Lock Up"

To ensure constant control over the Electronic Resources you are using and to prevent any opportunity for unauthorized use or disclosure, you must use the "stand up, lock up" practice of locking the Electronic Resources when stepping away, no matter how briefly, such that a password is required to resume use of the Electronic Resources.

D. Clean Desk Policy

Company Personnel should remove all Sensitive Personal Data from their workspaces when their workspace is unattended. Sensitive Personal Data should be contained in locked areas (e.g., file drawers, cabinets or rooms). Sensitive Personal Data should not be visible in your workspace to someone who may walk by or be meeting with you unless that person has reason to view the Sensitive Personal Data.

5.5 ENCRYPTION

A. Use of Encryption

The Company uses encryption to protect the confidentiality, integrity/authenticity, non-repudiation, and authentication of information where appropriate based on risk and the classification of the data using the classifications under the Company's Information Classification Policy.

B. Encryption Technical Standards and Approval of Encryption

You must never encrypt Company information unless you are in a position with the Company responsible for encrypting Company information and you are using Company approved encryption technology. All use of encryption must be approved by the Information Security Office prior to use. The Information Security Office will maintain technical standards for the use of encryption, including, but not limited to, file encryption, whole disk encryption, SSL/TLS encryption, and cryptographic certificates. All implementations of encryption must comply with the technical standard and must not be implemented without the formal review and approval of the Information Security Office.

C. Encryption Key Management

The Information Security Office is responsible for the management of all encryption keys. The generation, storing, archiving, retrieving, distributing, retiring and destroying of keys shall only be performed by the Information Security Office or the Cryptographic Key Custodians that the Information Security Office formally approves, oversees, guides and audits. All activity involving encryption keys shall be logged and audited.

5.6 Application Security

The Company will develop and document secure engineering principles and rules for applications or code developed to access, process, manipulate, or report Company information based on the classification level of the information. These rules will be applied to all code prior to that code accessing, processing, manipulating, or reporting the information. The Company will supervise the activity of outsourced development and the Information Security Office will monitor and audit this activity.

5.7 Monitoring

Company systems and facilities equipment are provided as a business tool. The Company retains the right to monitor all Electronic Resources, systems, equipment and physical areas of the business to protect the Company and Company Personnel and to ensure the appropriate use of the Company Electronic Resources. For more information regarding the Company's monitoring policy, please see the Company's Workplace Monitoring Policy.

5.8 Security and Privacy Incident Response Management

The Company has established a documented process to deal with incidents and you are responsible for reporting incidents as soon as possible in accordance with the Incident Reporting section found in this and in every policy of the Information Security Policies Framework.

The Information Security Office and the Global Privacy Office have jointly developed a Global Privacy and Security Incident Response Plan ("Incident Response Plan") to allow each team to efficiently and effectively respond to incidents and coordinate with each other, IS and other key stakeholders in the event of an incident. The Incident Response Plan is meant for only those Company Personnel who have a need to be involved in such incidents. The Incident Response Plan is not available for all Company Personnel.

All notifications to third parties regarding security incidents and/or potential data breaches must be approved by the leaders of the Information Security Office and Global Privacy Office.

5.9 Privacy and Data Protection Compliance

You are responsible for data protection compliance with the guidance of the Global Privacy Office and the Information Security Office. You are responsible for complying with the Company's Personal Data Protection Policy, GDPR Compliance Policy, CASL Compliance Policy and any other similar policies issued specific to compliance with applicable data protection laws.

5.10 Artificial Intelligence ("AI")

You are responsible for complying with the Company's Artificial Intelligence ("AI") Policy. This Policy will describe the Company's governance and principles surrounding artificial intelligence including outlining permitted and prohibited uses of it.

5.11 Records Retention and Records Disposal

You are responsible for complying with the Company's Data Minimization Policy, which includes the Company's Records Retention Schedule. This Policy will explain how long you should retain various types of records and how you should properly dispose of them. You are excepted to comply with all Data Minimization initiatives which will be communicated to you from time to time (for example, the Delete the Delete initiative or the email inbox and S, T and U drive clean-up).

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 EXCEPTION HANDLING

While every exception to a policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Personal Data Protection Policy
- Workplace Monitoring Policy

9 DOCUMENT INFORMATION

Document Name	Information Security Policy
Issue Date	January 1, 2025
Next Review Date	January 1, 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Craig White
Owner	Andrew Sheppard

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Nov. 1, 2010	First version issued
2.0	Nov. 1, 2011	Annual review
3.0	Jan. 1, 2013	Annual review – changed to 1/1 review cycle
4.0	Jan. 1, 2014	Annual review

5.0	Jan. 1, 2015	Annual review
6.0	June 1, 2016	Annual review
7.0	Jan. 1, 2017	Annual review - added training and education language to enforcement section; minor typos and wording changes
8.0	Nov. 18, 2018	Annual review – updated logo
9.0	Jan. 1, 2020	Annual review –used new template; revised significantly to accommodate new Information Security Program standards, Workplace Monitoring Policy; streamlined content to make it easier for readers to digest
10.0	Jan. 1, 2021	Annual review – minor wording changes and typos
11.0	Jan 1, 2022	Annual review – explained changes to the organization of the Privacy and Protection Team in IS (combination with data governance and master data management); added reference to new Global Privacy and Security Incident Response Plan; minor wording changes and typos
12.0	Jan 1, 2023	Annual review – minor typos and wording changes
13.0	Jan 1, 2024	Annual review – added clarification of information security incident to incident reporting section; added full list of Information Security Framework policies; updated definition of Electronic Resources; added definitions for Data Subject, Personal Data and Sensitive Personal Data; added Clean Desk Policy; added additional data handling information to the Information Classification section; added section on Artificial Intelligence; minor wording changes
14.0	Jan 1, 2025	Annual review – Updates to Incident Response and Scope sections consistent with changes made to all Information Security Framework policies; updated definition of Electronic Resources and Sensitive Personal Data and added definition for European Sensitive Personal Data; clarified definition of information assets and Personal Data to be defined collectively as “Protected Assets”; added AI Center of Excellence to Section 5.1, added requirement to comply with data minimization initiatives in Paragraph 5.11; other minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Information Classification Policy

Document ID:	AG-ISMS-POL-ICP
Version Number:	14.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Information Classification Policy (the “Policy”) is part of the Information Security Policies Framework and provides guidelines for classifying the Company’s Personal Data and information assets (collectively “Protected Assets”), and it establishes consistent security requirements for classifying, labelling, handling, and disposing of information in a secure manner.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them.

The Company needs your help in identifying those incidents and violations. An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) “**Company”** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", “our” or “Our” or "us" or "Us".

(2) “**Company Personnel**” means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company’s Protected Assets (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company’s systems or information. In this Policy, Company Personnel is also referred to as “You” or “you” or “Your” or “your”.

(3) "**European Sensitive Personal Data**" means information collected from or about individuals in Europe (collectively “Europe” for purposes of this Policy refers to the EEA countries, the UK and Switzerland) relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, as well as data concerning health or data concerning a person's, sex life or sexual orientation. In some European member states, it may also include information about a person's criminal convictions.

(4) **"Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(5) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(6) "**Sensitive Personal Data**" means collectively European Sensitive Personal Data, any type of Personal Data that is considered "sensitive" data under applicable data protection law and for all individuals, regardless of applicable data protection law, includes health data, biometric data, genetic data, an individual's account log-in, financial account, debit card, or credit card number when in combination with any required security or access code, password, or credentials allowing access to an account, immigration and citizenship status and social security numbers, driver's license numbers, or other state/national identification numbers and state/national identity documentation (such as passports).

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote locations). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 CLASSIFICATION TYPES, DESCRIPTIONS AND EXAMPLES

You are responsible for applying labels where feasible, abiding by labels and handling data, whether or not labelled, according to the requirements of this Policy. The Company has the following information classification types:

Classification Type	Security Level	Description	Examples
Restricted	**Maximum**	Highly sensitive information which, if accessed by an unauthorized person, could influence the Company's operational effectiveness, cause a serious breach of data protection laws, provide significant gain to a competitor or lead to a major drop in customer confidence.	• Controlled Unclassified Information ("CUI") (see Supplemental Policy regarding CUI) • Pending mergers and acquisitions • Passwords • Corporate-wide financial forecasting • System administrator passwords • Technical security control procedures • Confidential security incidents • Sensitive Personal Data (high volumes)
Highly Confidential	**High**	Any Personal Data protected by data protection statutes, any information protected by Company policies or contractual obligations, and non-public financial and business/strategic information regarding the Company. Loss of this type of information could cause a breach of data protection laws (for example, Sensitive Personal Data, regardless of volume) or lead to reputational or other harm to the Company.	• Personnel records • Personal Data (breach potential) • Customer and supplier contracts • Customer and Supplier confidential information • Proprietary source code • Financial forecasting • Strategic business plans • Information security risk assessments
Confidential	**Medium**	Default classification for all non-public information if it isn't classified otherwise. Used for information that is not particularly sensitive but is not generally released into the public	• Company policies • Non-sensitive technical specifications • Contract templates

		domain. Personal Data would be of a type that would not trigger a data breach if lost (e.g., basic applicant CV/resume data that does not include date of birth).	• Standard pricing information • Personal Data – no breach potential
Public	**Normal**	Information intended for release to the public or which is already publicly available. Disclosure of this type of information outside the Company would not cause any harm to the Company.	• Press releases • Service brochures and final marketing materials • Information on the Company's websites

5.2 HANDLING GUIDELINES – BY CLASSIFICATION TYPE

Classification Type	Handling Guidelines
Restricted	• For internal handling: should be disclosed only to a limited group of named individuals who are on a strictly need-to-know basis. • For external handling: should only be disclosed to parties who have signed a non-disclosure agreement or other confidentiality obligation with the Company, including appropriate data protection language if Personal Data or Sensitive Personal Data is involved.
Highly Confidential	Same as Restricted, except the size of the group of individuals may be, and is usually, larger (for example an entire department or type of role containing numerous employees).
Confidential	• For internal handling: may be disclosed to anyone inside the Company. • For external handling: may be shared on a need-to-know basis. Depending on the information, it may also be advisable to have a non-disclosure agreement or other confidentiality obligation in place.
Public	No restrictions.

5.3 STORAGE AND SAFEKEEPING GUIDELINES – BY CLASSIFICATION TYPE

Classification Type	Storage and Safekeeping Guidelines
Restricted	• When not in use, keep in locked drawers, cabinets, rooms or similar safe location. • When in use, maintain adequate security at all times (for example, cover up the information or turn documents over when unauthorized Company Personnel are likely to have sight of them). • When storing electronically, store in file share folders, share sites or other similar locations with access limited to only those authorized to access the information. • When storing in systems, only use systems approved by the Company.
Highly Confidential	Same as Restricted
Confidential	Make sure it is not accessible to unauthorized users, such as visitors who don't have a reason to access it.
Public	No restrictions.

5.4 Copying and Printing Guidelines – By Classification Type

Classification Type	Copying and Printing Guidelines
Restricted	When printing, use secure printing methods when available. Otherwise, retrieve from the printer immediately to avoid unauthorized persons gaining access. Do not leave copies unattended.
Highly Confidential	Same as Restricted
Confidential	Retrieve copies to avoid visitors and other outsiders who are unauthorized from gaining access.
Public	No restrictions.

5.5 Transmission Guidelines – By Classification Type

Classification Type	Transmission Guidelines
Restricted	• Have verbal conversations in secure locations that will avoid inadvertent disclosure to unauthorized persons. • When sending information by email, password protect the file and double-check your recipient addresses for the email prior to sending. Do not provide the password to the file in the email that contains the file. It is best to call the recipients to provide the password. Where possible, utilize encryption as appropriate to an email, or file or upload files or other information to an FTP or similar restricted mode of transmission.
Highly Confidential	Same as Restricted
Confidential	Be careful to double-check the addresses of all emails to avoid sending to the wrong recipients who may be inside or outside the Company.
Public	No restrictions.

5.6 Destruction and Disposal Guidelines – By Classification Type

Classification Type	Destruction and Disposal Guidelines
Restricted	• Dispose of printed copies using Company-provided shredding bins. Never put in a regular trash receptacle. • IS will be responsible for safely erasing any electronic media or electronically stored information.
Highly Confidential	Same as Restricted
Confidential	Same as Restricted
Public	Same as Restricted – You may use our shredding bins for all types of information. You may also use a standard trash receptacle or standard recycle bin.

5.7 SECURITY STANDARDS

The Information Security Office will maintain additional security standards governing each of the classification types that must be followed by specific roles in departments such as IS.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 EXCEPTION HANDLING

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Personal Data Protection Policy

9 DOCUMENT INFORMATION

Document Name	Information Classification Policy
Issue Date	January 1, 2025
Next Review Date	January 1, 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Craig White
Owner	Andrew Sheppard

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Nov. 1, 2010	First version issued
2.0	Nov. 1, 2011	Annual review
3.0	Jan. 1, 2013	Annual review – changed to 1/1 review cycle
4.0	Jan. 1, 2014	Annual review
5.0	Jan. 1, 2015	Annual review

6.0	June 1, 2016	Annual review
7.0	March 1, 2017	Annual review – Updated definition of Sensitive Personal Data and Electronic Resources; clarified some of the examples of types of information; added training and education language to enforcement section; minor typos and wording changes
8.0	Nov. 18, 2018	Annual review – updated logo
9.0	Jan 1, 2020	Annual review –used new template; changed content to be easier to digest by reader
10.0	Jan 1, 2021	Annual review – minor wording changes and typos
11.0	Jan 1, 2022	Annual review – clarified personal data types for classification levels; minor wording changes and typos
12.0	Jan 1, 2023	Annual review – updated definition of Sensitive Personal Data to match definition in Personal Data Protection Policy; minor typos and wording changes
13.0	Jan 1, 2024	Annual review - added clarification of information security incident to incident reporting section; added full ist of Information Security Framework policies; clarified that Confidential information is non-public; updated definition for Sensitive Personal Data; minor wording changes
14.0	Jan 1, 2025	Annual review – Updates to Incident Response and Scope sections consistent with changes made to all Information Security Framework policies; updated definition of Sensitive Personal Data and EU Sensitive Personal Data to “European” Sensitive Personal Data; clarified definition of information assets and Personal Data to be defined collectively as “Protected Assets”; other minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Workplace Monitoring Policy

Document ID:	AG-ISMS-POL-WMP
Version Number:	6.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Workplace Monitoring Policy (the "Policy") is part of the Information Security Policies Framework and gives guidance on how the Company Monitors its Company Personnel. The Company needs to conduct Monitoring of its Company Personnel for the following reasons:

- To protect Personal Data the Company processes as well as Company assets, confidential information of the Company and confidential information entrusted to it and other similar interests;
- To uphold our standards for security, conduct and quality control;
- To provide a workplace which is safe, supportive and inclusive; and
- To fairly and consistently apply our disciplinary and grievance policies.

The Company recognizes that these objectives must be balanced against the privacy of Company Personnel and that the Monitoring must be subject to robust governance to ensure the information gathered is held securely and used fairly.

The purpose of this Policy is to inform Company Personnel to what extent they can expect to be Monitored and to establish the governance that will apply.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, and any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(2) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's

information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(3) "**Electronic Resources**" means any (a) information technology equipment, devices or related equipment (such as servers, computers, laptops, desk phones, mobile phones, tablet PCs (e.g., iPad), thumb drives or other storage devices or multi-function printer/copier/scanner/fax machines); (b) electronic key fobs/cards; (c) internet and internet connections; (d) intranets; (e) network file shares (such as the Q:, S:, T:, U: or O: drives); (f) file sharing sites (such as Team Sites, OneDrive and SharePoint); (g) databases; (h) online subscriptions and services (such as WebEx or LinkedIn Recruiter); (i) applications, whether cloud or on-premise (such as Office 365, voice mail, PeopleSoft, Salesforce ("Connected') or Bullhorn); and (j) CCTV and any other similar resources of any kind each of which are (i) supplied by the Company to you for use for work-related purposes or (ii) not supplied by the Company to you, but are either: (a) used by you to connect to any Company network or (b) used in a way that relates to the Company's business and/or your work for or on behalf of the Company, whether intended or not. For purposes of this Policy, Electronic Resources do not include Company Personnel personal communications that do not relate to the Company's business and/or the Company Personnels' work for or on behalf of the Company and that are stored somewhere other than on the Company's systems, such as a personal secure website, private (not public) social media page, or personal emails provided by a third-party internet or email service provider.

(4) "**Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(5) "**Minor Infractions**" means behaviors or actions which do not (in isolation) constitute Misconduct, but which are contrary to Company guidelines, are examples of bad practice or could put the Company at risk.

(6) "**Misconduct**" means failure to abide by applicable Company policy or relevant enforceable standards, any breach of applicable law or any action or behavior that would constitute misconduct (or gross misconduct) under the Company's disciplinary policies, including but not limited to theft of confidential information of the Company or actions that may impair or interfere with the Company's business. Repeated failures to correct reported Minor Infractions may collectively constitute misconduct.

(7) "**Monitoring**" or "Monitor" means observation of Company Personnel, whether electronically or by other means, for the purposes of ensuring compliance of those Company Personnel with the policies and legal responsibilities of the Company.

(8) "**Monitoring Purposes**" are the purposes described in Section 5.1 of this Policy.

(9) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(10) "**Social Media**" means collectively forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as photos or videos), and without meaning to create an all-inclusive list, includes any of the following: Facebook, LinkedIn, X, TikTok, Pinterest, Instagram, YouTube, WeChat, WhatsApp, Snapchat, Tumblr, Reddit, Quora and Flickr and Company-maintained sites (such as Yammer, Viva Engage and Microsoft Teams chat).

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote location). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours, or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards and guidelines.

5.1 PURPOSES OF MONITORING

Company Electronic Resources are provided as a business tool. The Company retains the right to Monitor all Electronic Resources and physical areas of the business to:

- Protect the Company and Company Personnel, including Personal Data the Company processes and confidential information about the Company or entrusted to the Company;
- Ensure the use of the Company Electronic Resources and other resources and information assets are in compliance with applicable law;
- Monitor whether the use of the Electronic Resources or the Internet or Social Media is legitimate and in accordance with Company policy (including, but not limited to the Acceptable Use Policy and Social Media Policy) or applicable standards;
- Find lost emails, messages, postings, files or to retrieve emails, messages, postings, or files lost due to computer failure or other system issues;
- Utilize data discovery technology for purposes such as litigation discovery, data discovery for Data Subject requests or data discovery as a supplement to data mapping efforts to locate and categorize data for further appropriate handling;
- Investigate actual, alleged or suspected Misconduct, including assisting law enforcement agencies; and
- Comply with any legal obligation to which the Company is subject including, where applicable, contractual obligations.

The exact purposes for which Monitoring may be conducted, and the parameters of such Monitoring, may vary between jurisdictions to ensure such activities comply with applicable law. All the purposes set forth in this section 5.1 are collectively referred to in this Policy as the "**Monitoring Purposes**".

This Policy is not intended to preclude or dissuade employees from engaging in activities protected by state or federal law, including the National Labor Relations Act, such as discussing wages, benefits or other terms and conditions of employment or legally required activities.

5.2 METHODS OF MONITORING

This section 5.2 describes the Company's global default position on how routine Monitoring is conducted.

In addition to the methods described in this section, the Company reserves the right to use any lawful method of Monitoring for the Monitoring Purposes, including, without limitation, when investigating actual, alleged or suspected Misconduct. Such investigations will be made within the limits described in this Policy, and in accordance with applicable laws.

Portions of the Company may issue local standards which limit or clarify the extent of Monitoring which they provide to account for factors such as local applicable law, business needs or the means of Monitoring available. If in doubt as to whether any such standards apply to you or the Company you work for, please consult that Company's Global Privacy Office or your applicable Employee/Staff Privacy Notice.

A. CCTV

Where it is permitted by local law, and considered a proportionate measure by the Company, Company Personnel may be Monitored by CCTV whilst on Company premises.

B. ELECTRONIC RESOURCES

By default, any and all information contained within Electronic Resources may be Monitored by the Company. Using any automated or non-automated means, these communications and information, and the Electronic Resources, may be Monitored, accessed, retrieved, copied, stored, read, seized and/or disclosed by, or at the direction of, the Company or law enforcement for any lawful purpose, subject to the Company's Government Intelligence Data Request Policy and Procedure.

As such, you must have no expectation of privacy in any use of Electronic Resources or in any information or communications transmitted to or from, received or printed from, or created, stored or recorded on the Electronic Resources, including situations involving personal use. This includes, without limitation, email (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages, and internet and social media posting and activities, log-ins, recordings, and other uses of the Electronic Resources as well as keystroke capturing and other network monitoring technologies.

This is true regardless of the labelling of the information (for example, as "personal" or "private"), the use of encryption, the deletion of the information or communications, or any other factor. Do not use the Electronic Resources for any personal matter that you desire to be kept private or confidential from the Company.

C. SOCIAL MEDIA ACTIVITY

The Company may Monitor your Social Media activity (including use outside of working hours and/or without the use of Electronic Resources) to minimize risks presented by the use of Social Media, as detailed in the Company's Social Media Policy. Any Monitoring of Social Media will be in compliance with this Policy and the Social Media Policy. Such Monitoring will generally not take place at an individual level except:

- During an investigation into suspected Misconduct; or
- Your level of seniority or public exposure with the Company make routine Monitoring of your Social Media a reasonable precaution.

D. BRING YOUR OWN DEVICE (BYOD) PROGRAMS

The Company's IT/IS function may operate BYOD programs which allow you to use your personal devices, such as computers, smartphones and tablets, for business purposes. Participation in BYOD programs will be voluntary but may require you to grant the Company (and/or the Company's suppliers involved in the program) with a degree of access to your device and its contents ("**Permissions**") to maintain security. In most of our jurisdictions, we do not provide cell phones, but we will always provide a laptop. If you wish to also access email and other approved apps on your mobile device, you may voluntarily participate in the BYOD program. Before participating in BYOD programs, you should ensure you understand and accept the Permissions required.

For example, the Permissions required under the Company's BYOD Program include:

- The ability to remotely lock your device or delete information on it;
- Granting access to information about the device (e.g., operating system and version, device make and model, device unique identifying number) which could be used to personally identify you as the device's user; and/or
- Granting access to information generated by the device (such as location services or usage logs) which reveals information about your behavior that would not otherwise be available.

The Company will implement appropriate technical and organizational measures with regards to the Personal Data collected for the purposes of the BYOD Program. To learn more about our Company's BYOD Program, please see the Company's BYOD Policy.

5.3 SAFEGUARDS AND CONTROLS

A. ACCESS TO MONITORING INFORMATION

Monitoring practices are overseen by the Company's Information Security department.

Systems are implemented to automate Monitoring where viable to ensure real-time protection and minimal human intervention. However, the Company may need to Monitor systems manually from time to time to protect the Company.

Access to Monitoring is controlled and limited to trained and designated administrators to ensure an acceptable level of confidentiality and privacy.

B. MISCONDUCT AND MINOR INFRACTIONS

Any Misconduct of employees detected through Monitoring (whether routine Monitoring or during an investigation) will be dealt with in accordance with the Company's usual HR processes and procedures relating to disciplinary matters, including those processes and procedures set out in the applicable Company Employee Handbook.

Monitoring may also reveal behavior or actions which do not (in isolation) constitute Misconduct, but which are contrary to Company guidelines, are examples of bad practice or could put the Company at risk ("**Minor Infractions**").

Minor Infractions detected may be reported to you and/or your manager. Note that repeated failures to correct reported Minor Infractions may collectively constitute Misconduct.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 Exception Handling

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 Supporting Documents

- Acceptable Use of Electronic Resources Policy
- Bring Your Own Device ("BYOD") Policy
- Social Media Policy

9 Document Information

Document Name	Workplace Monitoring Policy
Issue Date	01, January 2025
Next Review Date	01, January 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Christen Grapes
Owner	Maureen Dry-Wasson

10 Version History

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	1 January 2020	First version – replaces monitoring sections of Acceptable Use of Electronic Resources Policy; BYOD Policy and Social Media Policy
2.0	1 January 2021	Annual review – minor wording changes and typos
3.0	1 January 2022	Annual review – minor wording changes and typos
4.0	1 January 2023	Annual review – updated definition of Social Media to match changes made in Social Media Policy; clarified that data discovery technology is a monitoring purpose; minor typos and wording changes
5.0	1 January 2024	Annual review - Added additional explanation for incident reporting; added full ist of Information Security Framework policies; minor wording changes.
6.0	1 January 2025	Annual review –Updated Incident Reporting and Scope sections for clarifying wording changes made to all Information Security Framework Policies; updated Social Media definition for changes in the names of

	some platforms; updated Electronic Resources definition to clarify what does not count as an Electronic Resource; updated BYOD section to clarify the voluntary nature of that program; other minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Social Media Policy

Document ID:	AG-ISMS-POL-SMP
Version Number:	14.0
Issue Date:	01 January, 2025
Next Review:	01 January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Social Media Policy (the “Policy”) is part of the Information Security Policies Framework and explains how the Company deals with Social Media and your usage of Social Media.

The Company welcomes the growing use of Social Media and recognizes that Social Media provides unique opportunities to participate in interactive discussions and share information on particular topics, all of which can drive business and support professional and personal development. However, at the same time, your use of Social Media can pose risks to the Company’s confidential and proprietary information and reputation and can jeopardize its compliance with legal obligations. This Policy has been created to minimize these risks, avoid loss of productivity and ensure that our IS resources and communications systems are used only for appropriate business purposes.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) “**Company”** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", “our” or “Our”, or "us" or "Us".

(2) “**Company Personnel**” means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company’s information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company’s systems or information. In this Policy, Company Personnel is also referred to as “You” or “you” or “Your” or “your”.

(3) "**Company Social Media Account**" means any Social Media account that is used exclusively for business purposes to interact with any of the Company's former, current or potential contractors, candidates, clients, customers, vendors, suppliers or the general public,

regardless of whether you or someone else within the Company has created the account. Various roles in the Company are involved with operating Company Social Media Accounts. See Section 5.3 for more information on Company Social Media Accounts.

(4) "**Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(5) "**Multi-Use Account**" means that if you are a recruiter for the Company, whether for internal or external recruiting, or your role in the Company involves providing thought leadership or marketing content through Social Media, the Company acknowledges that you may utilize Social Media (such as LinkedIn, X, Instagram or Facebook) as part of your recruitment or thought leadership efforts on behalf of the Company and that such accounts may be used for both personal and work purposes, so such accounts are referred to as a "Multi-Use Account". See Section 5.2 for more information on Multi-Use Accounts.

(6) "**Social Media**" means collectively forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as photos or videos), and without meaning to create an all-inclusive list, includes any of the following: Facebook (Meta), LinkedIn, X, TikTok, Pinterest, Instagram, YouTube, WeChat, WhatsApp, Snapchat, Tumblr, Reddit, Quora and Flickr and Company-maintained sites (such as Yammer, Viva Exchange and Microsoft Teams chat).

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote location). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 DO'S AND DON'TS OF SOCIAL MEDIA USE

The following are Do's and Don'ts regarding your use of Social Media:

DO	DON'T
Comply with Our Policies - If your post would violate any of the Company's policies in another forum it will also violate them in an online forum.	
Negative Post Reporting - Report negative Social Media posts or accounts that could potentially harm the reputation of the Company to your Marketing Department and let the Marketing Department, in consultation with Human Resources and/or Legal where needed, respond to any negative posts.	**Offensive/Discriminatory/Defamatory Content –** Don't post content or provide comments to the posts of others that could be considered offensive, discriminatory, defamatory, harassing, insulting, violent or obscene. Don't use a messaging capability to harass, insult or annoy others.
Common Sense Usage - Use Social Media responsibly by exercising common sense, writing knowledgeably, and striving to be accurate and professional. If in doubt, do not post.	**Use Social Media to Discriminate-** Don't use Social Media to discriminate against or exclude anyone including without limitation, potential applicants or other Company Personnel.
Privacy Settings - Ensure that your privacy settings on Social Media accurately reflect your intentions.	**Unlawful –** Don't violate any laws or regulations or any platform or website's Terms of Use. For example, don't use photographs taken by someone else or other copyrighted or trademarked content, unless you have appropriate permission and provide appropriate credits.
Product/Service Endorsement Disclosure - If you endorse Company products or services, you must clearly and conspicuously disclose your relationship to the Company.	**Misrepresentations –** Don't misrepresent your identity or your ability to speak on behalf of the Company. Don't misrepresent your identity or your ability to speak on behalf of the Company. Also, avoid postings that contain known misrepresentations, are deceptive, or misleading. If in doubt, do no post.
Precautions to Prevent Identity Theft - Take the necessary precautions to prevent identity theft as that could also jeopardize the Company's assets/resources. Some examples of precautions include: • Provide only basic information on Social Media; • Be cautious about providing information like date of birth, place of birth or any such personal information that could be used to steal your identity; and • Don't use passwords used to access Company systems, resources or	**Disclosure of Confidential Information-** Don't directly or indirectly disclose Company confidential information (for example, business strategies and goals, marketing plans, financial information and information about clients and candidates).

<table>
<tr><td>applications as passwords for Social Media.</td><td></td></tr>
<tr><td>Personal Use Limitations - Limit use of Social Media for personal purposes to outside of normal work hours or during lunch breaks to limit the impact on your productivity.</td><td>Require Disclosure of Credentials – Don't request or require an applicant or Company Personnel to disclose his/her/their personal Social Media log-in credentials; don't reject an applicant or discipline or terminate Company Personnel for failure to do so, except as permitted by applicable law.</td></tr>
<tr><td rowspan="2">Personal Views Statements – Clearly indicate in your Social Media postings that it is your own/personal views and not the views of the Company, unless you have been authorized to speak on behalf of the Company.</td><td>Unauthorized Access – Don't attempt to gain unauthorized or unlawful access to someone else's Social Media account.</td></tr>
<tr><td>Violate Agreements – Don't use Social Media in a manner that would violate the agreements that the Company has in place with its employees, customers, service providers or other business partners.</td></tr>
<tr><td>Approval for Postings- Do let people who are being photographed clearly know that their image may be used in Social Media, and let them have a chance to choose not to be featured.</td><td>Do not film your personal Social Media content on work premises, including lunch rooms, break rooms/areas and the parking lot</td></tr>
<tr><td rowspan="3">Protect Customers, Suppliers, and other Business Partners – Do not cite or refer to our customers, suppliers or other business partners, identify them by name or reveal any confidential information related to them without getting their explicit permission in advance as well as advance permission from the Company. Also, do not disclose or conduct business with a customer, supplier or business associate in an online forum.</td><td>Plagiarize – Don't plagiarize information; all information must be properly attributed to relevant sources.</td></tr>
<tr><td>Chain Letters/Spam – Don't circulate chain letters or spam to other people.</td></tr>
<tr><td>Company Policy Violation – Don't violate any Company policies.</td></tr>
</table>

5.2 MULTI-USE ACCOUNTS

A. What is a Multi-Use Account?

If you are a recruiter for the Company, whether for internal or external recruiting, or your role with the Company involves providing thought leadership content through Social Media, the Company acknowledges that you may utilize Social Media as part of your recruitment or thought leadership efforts on behalf of the Company and that such accounts may be used for both personal and work purposes (such Social Media accounts are referred to as a "Multi-Use Account" as noted in the Definitions section).

B. What do I need to do if I operate a Multi-Use Account?

If you operate a Multi-Use Account, you must agree to the following:

- **No Ownership by Company but Must Adhere to Policy -** Except where permitted by applicable law, the Company does not own Multi-Use Accounts and will not request your log-in information or passwords; however, if you elect to use a Multi-Use Account, your use of that account is subject to this Policy.
- **Follow OpCo Guidelines and Attend Training -** You must follow any guidelines issued by your Operating Company regarding the use of Multi-Use Accounts and attend any required training. Without limitation, this includes that in using Multi-Use

Accounts, you must position the Company in accordance with the Company's brand and strategic marketing standards, which are managed by the Marketing departments.

- **Clearly and Conspicuously Acknowledge Association with Company -** If you are posting/publishing thought leadership that was created with or by the Company, the post/publish must clearly and conspicuously acknowledge an association with the Company. For example, the post should contain a statement such as "I work for Allegis Group." The disclosure should be well-placed so it can be easily noticed.
- **Enter Information in Company Database -** You must enter into the appropriate database for your Operating Company (for example any Company "CRM", or Client Relationship Management system, like Connected or Bullhorn, or any Company "ATS", or Applicant Tracking System, like Connected or Bullhorn) any contact information regarding potential or current candidates or clients from your Multi-Use Account. Information in the Company's databases is considered confidential information of the Company.
- **Delete Content –** You agree to delete any content that violates this Policy.

5.3 COMPANY SOCIAL MEDIA ACCOUNTS

A. What is a Company Social Media Account?

A "Company Social Media Account", as noted in the Definitions section, means any Social Media account that is used exclusively for business purposes to interact with any of the Company's former, current or potential contractors, candidates, clients, customers, vendors, suppliers or the general public, regardless of whether you or someone else within the Company has created the account. Various roles in the Company are involved with operating Company Social Media Accounts (for example and without limitation, a Company LinkedIn, Facebook or Instagram account).

B. What do I need to do if I Operate a Company Social Media Account?

If you operate a Company Social Media Account, you must agree to the following:

- **Sign Social Media Account Ownership Agreement -** Sign the Company's Social Media Account Ownership Agreement if you are involved in using Company Social Media Accounts and provide it to the Company Personnel responsible for website development or as otherwise directed.
- **Obtain Prior Authorization -** Don't create or operate any Company Social Media Accounts without prior authorization from the leaders of your OpCo's Marketing Department.
- **Provide Log-in Credentials to Company and Protect Them** - Provide any log-in credential information to the Company Personnel responsible for website development for Company Social Media Accounts and protect the log-in credential information as Restricted information under the Company's Information Classification Policy.
- **Follow OpCo Guidelines and Attend Training -** Follow any guidelines issued by your Operating Company regarding the creation and maintenance of Company Social Media Accounts and attend any required training.

5.4 SOCIAL MEDIA MONITORING

The Company may monitor Social Media to validate compliance with this Policy. Notwithstanding this, the Company follows all applicable laws related to personal Social Media use of employees and job applicants. Regarding personal or Multi-Use Social Media accounts, the company will not, unless a legal exception applies, require or request that employee or job applicants do any of the following: disclose login credentials, access an account in such a way that allows the Company to observe the account's contents, add any person to the account's

contact list or change the account's privacy settings. The Company will not take adverse action against any employee or job applicant for failing to engage in the above actions.

Please see the Company's Workplace Monitoring Policy for additional information regarding how the Company monitors Social Media.

5.5 Employee Separation and Role Changes and Social Media Issues

If you separate from employment or change your role with the Company such that the role change impacts your involvement in Company Social Media Accounts or Multi-Use Accounts, you must:

- **Update Your Social Media Profile -** You must update your Social Media profile to accurately reflect your involvement with or separation from the Company.
- **Close/Transition Company Social Media Accounts -** Company Social Media Account users must close or transition the account to appropriate Company Personnel as directed by the Company.
- **Cease Using Multi-Use Accounts for Company Business -** You must cease using any Multi-Use Accounts for the purpose of Company business.

5.6 Conduct Not Prohibited by this Policy

This Policy is not intended to preclude or dissuade employees from engaging in activities protected by applicable law, including for those Company Personnel in the United States, the National Labor Relations Act, such as discussing wages, benefits or other terms and conditions of employment or legally required activities.

6 Enforcement

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 Exception Handling

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Information Classification Policy
- Workplace Monitoring Policy

9 DOCUMENT INFORMATION

Document Name	Social Media Policy
Issue Date	January 1, 2025
Next Review Date	January 1, 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Christen Grapes
Owner	Maureen Dry-Wasson

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Nov. 1, 2010	First version issued
2.0	Nov. 1, 2011	Annual review
3.0	Jan. 1, 2013	Annual review – changed to 1/1 review cycle
4.0	Jan. 1, 2014	Annual review
5.0	Jan. 1, 2015	Annual review
6.0	June 1, 2016	Annual review
7.0	March 1, 2017	Annual review - Added ceasing use of Multi-Use Accounts for company purposes following separation or change in role; added training and education language to enforcement section; minor typos and wording changes
8.0	Nov. 18, 2018	Annual review – updated logo
9.0	Jan. 1, 2020	Annual review – updated to new template; revised content to make it more digestible for reader
10.0	Jan. 1, 2021	Annual review – added notation to not use Company system passwords for Social Media; minor typos and wording changes
11.0	Jan. 1, 2022	Annual review – minor typos and wording changes
12.0	Jan. 1, 2023	Annual review – changed definition of Social Media Account to include interacting with the “general public”; revised the definition of Social Media to streamline and update the definition to current Social Media examples; added approval for postings to “Do’s” and not filming Social Media on work premises; minor typos and wording changes
13.0	Jan. 1, 2024	Annual review - Added additional explanation for incident reporting; added full ist of Information Security Framework policies; minor wording changes.
14.0	Jan. 1, 2025	Annual review – Changes to Incident Reporting and scope section consistent with changes made in all Information Security Program policies; updated Social Media definition for changes in names of platforms; added compliance with policies and protect customers, suppliers and business partners as “Do” activities; clarified that when acknowledging association with the company it must be “clear” and “conspicuous”; added clarity around activities the Policy was never meant to authorize (i.e., access to a personal social media account – language added to Par. 5.4 and new Par. 5.6 added to clarify it is not

	meant to dissuade labor organizing activities); other minor wording changes

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Personal Data Protection Policy

Document ID:	AG-ISMS-POL-PDP
Version Number:	14.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Personal Data Protection Policy (the "Policy") is part of the Information Securities Policies Framework and requires you to ensure that the Personal Data we collect, use, share or disclose is handled in accordance with applicable data protection laws. We treat compliance with our data protection obligations seriously. This is why we have developed our Global Privacy Principles (which describe the standards that we apply to protect Personal Data) and this Policy.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, and any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in any investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(2) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(3) "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

(4) "**European Sensitive Personal Data**" means information collected from or about individuals in Europe (collectively "Europe" for purposes of this Policy refers to the EEA countries, the UK, and Switzerland) relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, as well as data concerning health or data concerning a person's sex life or sexual orientation. In

some European member states, it may also include information about a person's criminal convictions.

(5) "**Information Security Policies Framework"** means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(6) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(7) "**Sensitive Personal Data**" means collectively European Sensitive Personal Data, any type of Personal Data that is considered "sensitive" data under applicable data protection law and for all individuals regardless of applicable data protection law, includes health data, biometric data, genetic data, an individual's account log-in, financial account, debit card, or credit card number when in combination with any required security or access code, password, or credentials allowing access to an account, immigration and citizenship status, and social security numbers, driver's license numbers, or other state/national identification numbers and state/national identity documentation (such as passports).

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility, when accessing any Company systems or networks (including, for example, when working from home or other remote location), or when they otherwise have access to Company Personal Data. Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards and guidelines.

5.1 COMPANY USE OF PERSONAL DATA

The use of Personal Data is critical to the Company in order to:

(a) Provide services to customers;
(b) Promote services to prospective customers;
(c) Recruit Company Personnel as part of our business operations; and
(d) Carry out internal management and administration of the Company and its employees, including working with vendors.

From start to finish, these activities involve the use of Personal Data, which is subject to applicable data protection laws. It is critical that our job seekers and candidates, employees, customers and vendors are confident that their Personal Data is safe and that the Company will use it in accordance with applicable data protection laws.

In particular, the Company's GDPR Compliance Policy applies to any processing of Personal Data which is under the scope of the General Data Protection Regulation ("GDPR"). As detailed in the GDPR Compliance Policy, this can include processing by parts of the Company which are not incorporated or operating in Europe.

5.2 TRAINING

All Company Personnel will receive mandatory general data protection training over an annual cycle. Auditable records of completion will be maintained to monitor attendance. Additional function-specific training will be provided for teams and departments which regularly process Sensitive Personal Data or whose functions otherwise present significant data protection risks. The content, mode of delivery and frequency of training programs will be regularly reviewed to monitor its effectiveness in providing sufficient guidance.

5.3 COMPANY GLOBAL PRIVACY PRINCIPLES

The following Company Global Privacy Principles apply to how you should collect, use and disclose or share Personal Data.

A. Transparency

#	Privacy Principle	What Does It Mean?	What Can You Do?
1	**Transparency**	Being open, honest and fair.	• **Privacy Notices.** Provide Privacy Notices at the time of collection of information or as soon as practicable after collection, so individuals know who we are, what Personal Data (including what Sensitive Personal Data) we collect and how we use, disclose and share it. For example, this includes a Privacy Notice to our employees at onboarding and when we make updates, and a Privacy Notice to website visitors, job seekers, candidates, suppliers and customers posted on our websites to explain how we will collect, use, disclose and share their Personal Data. This includes providing our California Notice at Collection or other Privacy Notice when you interact with individuals offline (for example on the telephone or in person at our offices or other locations) by providing individuals with information about where it is posted online. In addition, this includes providing appropriate notices as required by applicable data protection law regarding use of artificial intelligence or other required notices.

			• **Personal Data from Third Parties.** If third parties provide Personal Data to us, check that they have provided suitable privacy notices to the individuals concerned to explain that we will be handling their Personal Data in the ways we intend.

B. Specified and Lawful Purpose

#	Privacy Principle	What Does It Mean?	What Can You Do?
2	**Specified and Lawful Purpose**	Tell individuals the purposes for collecting, using or sharing Personal Data and then use it only for those specific purposes, which must be lawful purposes. Obtain consent where required by law.	(1) **Purpose Limitations.** The applicable Privacy Notice must explain the purpose for collecting, using, disclosing and sharing Personal Data and Sensitive Personal Data. These notices are drafted by the Global Privacy Office, but it is your obligation to notify the Global Privacy Office if you see gaps between how you are handling Personal Data and the applicable Privacy Notice by reporting a privacy incident and by following the steps in Section 2 for reporting an incident. (2) **Consent and Other Requirements.** You must obtain consent according to the applicable legal consent requirements when collecting, using, disclosing or sharing certain Personal Data. Additionally, consent is required when we are collecting biometric data from any individual. In some jurisdictions, you may need consent, or you may need to take other steps when collecting certain types of Personal Data, particularly Sensitive Personal Data as explained in the Sensitive Personal Data section of this Policy. You should use Personal Data for the purpose for which you received it. If you intend to use it for a secondary purpose, where required by applicable data protection law, you must first obtain consent. (3) **Lawful.** You must never collect Personal Data in a way that is unlawful or where we don't have the appropriate lawful basis for jurisdictions, like Europe, Singapore, Japan, or China, that require a lawful basis for processing.

C. Accurate, Complete and Up-to-Date

#	Privacy Principle	What Does It Mean?	What Can You Do?
3	**Accurate, Complete and Up-to-Date**	We must keep Personal Data accurate, complete and up-to-date to ensure data quality. Processing inaccurate information about an individual can be harmful to individuals and to us.	• **Encourage Active Changes.** Actively encourage individuals including employees, job seekers and candidates, customers and vendors to update their Personal Data with the Company, either manually and/or by automated reminders. For example, when you are communicating with individuals, invite them to notify you of any changes to their Personal Data. • **Making Changes.** When we learn of any changes to Personal Data that individuals cannot change themselves (for example because they can't access the system where the data is

			stored), you should make the appropriate changes.

D. Relevant

#	Privacy Principle	What Does It Mean?	What Can You Do?
4	**Relevant**	We must only collect Personal Data that is necessary for the purpose(s) for which we are collecting it. We should not collect data we do not need or that is excessive. We should always apply the minimum necessary rule to the collection and sharing of all Personal Data.	• **Don't Collect Outside of Communicated Purpose.** When collecting Personal Data from individuals, do not collect any Personal Data that isn't necessary to achieve the purposes that are listed in the appropriate Privacy Notice. • **Don't Share More Personal Data Than is Needed.** When disclosing Personal Data, only disclose the Personal Data needed to accomplish the intended purpose. For example, if you are celebrating birthdays in a department, you only need to disclose the month and date of someone's birthday and not the birth year. Additionally, when disclosing spreadsheets of information, remove any columns that aren't needed by the recipient (for example don't include SSN unless the recipient needs that information).

E. Retain Only As Needed

#	Privacy Principle	What Does It Mean?	What Can You Do?
5	**Retain Only As Needed**	You should only keep Personal Data where there is a legal or business need to do so and not just because it might be useful one day.	• **Data Minimization Policy/Records Retention.** You must follow the Company's Data Minimization Policy, which includes the Records Retention Schedule which outlines how long you should keep various types of records and how you should destroy them when no longer needed. • **Customer Retention Requirements.** If a customer requires us in a written contract to retain Personal Data, we must retain such Personal Data according to the customer's reasonable and legal requirements, and in the interests of the Data Subjects. Conversely, if a customer requires us in a written contract to return or delete Personal Data we have collected from the customer, we must follow the customer's instructions, subject to retaining any customer data that we have a legal right to maintain. You should consult with the Global Privacy Office as needed.

F. Respect Data Subject Rights

#	Privacy Principle	What Does It Mean?	What Can You Do?
6	**Respect Data Subject Rights**	You must comply with Data Subject rights, which vary by applicable law. These rights include, for example, rights to access, delete and correct data, as well as the right to unsubscribe from communications they receive from us. This also includes the right for Data Subjects to submit questions, concerns and complaints regarding the handling of their Personal Data and to be protected from discrimination for exercising their Data Subject rights.	• **Questions and Complaints.** We must reply to questions, complaints and requests concerning our processing of Personal Data in a reasonable period of time and in accordance with applicable law. You should report it as an incident as outlined in Section 2 if you become aware of a complaint related to a Data Subject request so that the Global Privacy Office can respond. • **Unsubscribe Requests and Preferences.** Individuals have the right to unsubscribe from certain communications we send by email and by text, and they have the right to tell us how they want us to communicate with them (for example, by text or about certain topics but not others). You must comply with any procedures the Company provides related to your role in the processing of such unsubscribe requests and honor any preferences. This may include unsubscribing from marketing communications or other types of communications where we are required by applicable law to provide a right to unsubscribe (for example, under CAN-SPAM in the US, CASL in Canada or the e-Privacy Directive in the EU) or not communicating by text because we don't have the required consent or the Data Subject has indicated a preference for email communications. • **Data Subject Rights Requests.** If you receive a request from a Data Subject who wants to exercise his or her rights under applicable data protection law (for example, a right to access or delete Personal Data or object to processing), you should immediately forward the request to the Global Privacy Office by reporting an incident as outlined in Section 2. The Global Privacy Office will handle all Data Subject requests. • **Intelligence Data Requests.** If you receive a request from a government for access to any Personal Data we hold for purposes of national security intelligence, you must report that immediately to the Global Privacy Office by reporting an incident as outlined in Section 2. The Global Privacy Office will handle all such requests as per the Company's Government Intelligence Data Request Policy and Procedures.

			• **Opt-out of Sales of Personal Data/Opt-out of Targeted Advertising and Opt-out of Profiling.** Several US privacy laws require that we respect a Data Subject's right to opt-out of our sale of Personal Data, to opt-out of targeted advertising and opt-out of profiling. The Global Privacy Office is responsible for tracking these requirements and implementing compliance procedures. The Global Privacy Office has determined that the only time we "sell" Personal Data under US privacy law is when we utilize targeted advertising cookies. We only use targeted advertising cookies when a Data Subject opts-in to our use of them, and at all times, a Data Subject has the right to opt-out. The Global Privacy Office has determined that we do not currently engage in any profiling as defined under applicable data protection law. • **Automated Decision-making and AI.** There are data protection laws related to automated-decision-making and artificial intelligence that vary by jurisdiction and are fast evolving. The Global Privacy Office in collaboration with the Company's AI Center of Excellence tracks these laws and has processes implemented to identify any such activities and respond with appropriate steps, including but not limited to providing notices, performing risk assessments and audits, and other steps required or advisable under law to ensure any AI is utilized responsibly. For more specific information regarding artificial intelligence, please see our AI Policy. • **Compliance with Applicable Data Protection Laws.** There are US state and worldwide data protection laws that provide various Data Subject rights. Please see specific policies like the CASL Policy and the GDPR Compliance Policy for additional information regarding specific laws. Not every data protection law has a specific, dedicated policy; however, the Company is committed to complying with all applicable data protection laws. If you have any specific questions regarding applicable data protection laws, please contact the Global Privacy Office by sending an email to privacyofficer@allegisgroup.com.

G. Security Measures

#	Privacy Principle	What Does It Mean?	What Can You Do?
7	**Security Measures**	All Personal Data must be kept secure. We must apply appropriate technical and organizational measures to protect Personal Data from unauthorized or unlawful processing or disclosure and from accidental loss, destruction or damage. When considering the level of security, we will take into account: (1) the state of technological development, (2) the cost of implementing any measures, (3) the harm that might result from a breach of security and (4) the nature of the Personal Data protected.	• **Information Security Policy.** You must observe the requirements set out in the Information Security Policy. This Policy describes steps you can take to apply the appropriate technical and organizational measures to protect Personal Data. • **Information Classification Policy.** You must observe the requirements set forth in the Information Classification Policy. This Policy describes how to appropriately label and then protect Personal Data. • **Disclosing Personal Data with Third Parties.** If you disclose Personal Data to third parties or have a third party who will collect, store or use Personal Data that we have provided (for example vendors), you must ensure that we have the appropriate data protection terms in our written contract with those third parties. Please work with the Allegis Group Procurement team and Allegis Group Third Party Risk Management Team and/or your OpCo Privacy Analyst to make sure we have the appropriate data protection language in contracts and the appropriate vetting of third parties who process Personal Data or provide Personal Data to us.

H. International Transfers

#	Privacy Principle	What Does It Mean?	What Can You Do?
8	**International Transfers**	We seek to comply with all global requirements regarding transfers of Personal Data across country borders.	• **Transfers from Europe to Outside Europe.** You should not transfer Personal Data across country borders (most notably outside Europe) unless appropriate steps have been taken. For transfers from Europe to jurisdictions that are outside Europe the Company has taken the following steps to allow for such transfers: ○ All entities within the Company worldwide have signed a Global Data Transfer Agreement that is compliant with European law (the 2021 Standard Contractual Clauses) from any Allegis Group entity to any other Allegis Group entity (for instance our companies in Germany sending Personal Data to our companies in the Philippines or the US). The Global Privacy Office maintains this document. ○ For transfers involving our vendors/suppliers or our customers, utilize appropriate transfer mechanisms (e.g., Standard Contractual Clauses) and supplementary measures, where necessary. • **EU-US Data Privacy Framework ("DPF"); UK Extension to the EU-US DPF and Swiss-US DPF (collectively referred to as "DPF").** These new frameworks replaced Privacy Shield. The frameworks were respectively developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for Personal Data transfers to the United States from Europe while ensuring data protection that is consistent with European law. We maintained our Privacy Shield certification and have transitioned it to a DPF certification which means that transfers of Personal Data from Europe to the US are considered "adequate" under GDPR (an alternative to signing the Standard Contractual Clauses). To provide evidence of our certification to outside parties, provide this link and tell them to search for "Allegis Group" in the search bar: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000XZY0AAO&status=Active • **China.** Transfers of Personal Data outside of China is subject to strict rules including volume

			limits, Data Subject consent and may require impact assessments and Standard Contractual Clauses. Please coordinate with the Global Privacy Office for any such transfers. • **Japan.** Transfers from Japan generally require Data Subject consent and a contract such as a Data Protection Agreement. • **Other Transfers.** There are no restrictions related to transfers of Personal Data from the US to outside of the US. Many countries require cross border transfers to be accompanied by legally enforceable obligations to the receiving party. Allegis Group uses Data Protection Agreements and the Third Party Risk Management (TPRM) process to meet such requirements. There may be restrictions or specific requirements related to transfers of Personal Data from Canada, South American countries, Latin American countries and APAC countries (for example, Singapore and New Zealand), so if you know you will be transferring Personal Data across borders and you need assistance, please send an email to the Global Privacy Office at privacyofficer@allegisgroup.com.

I. Sensitive Personal Data Precautions

#	Privacy Principle	What Does It Mean?	What Can You Do?
9	**Sensitive Personal Data Precautions**	Some laws provide special and stricter protections for specific types of Personal Data that we refer to as Sensitive Personal Data. We need to follow such requirements related to protecting Sensitive Personal Data. Each law may define Sensitive Personal Data differently.	• **More Stringent Protection.** When you are handling Sensitive Personal Data, your standard of care should be higher. • **Consent, Privacy Impact Assessments or Other Requirements.** Where required by law, if you need to obtain consent in order to collect, use or disclose Sensitive Personal Data, you must follow such requirements. For example, you must obtain explicit consent in order to collect or use European Sensitive Personal Data (for more details see the GDPR Compliance Policy). In addition, you must obtain consent to collect Sensitive Personal Data under certain US state privacy laws (as defined under each applicable US state law). Several worldwide data protection laws also require privacy impact assessments when Sensitive Personal Data is involved. The Global Privacy Office tracks the requirements for each

			of these laws and will handle making sure these requirements are met where required under law.

J. Customer Instruction Compliance

#	Privacy Principle	What Does It Mean?	What Can You Do?
10	**Customer Instruction Compliance**	Sometimes we collect, hold and use Personal Data on behalf of our customers (where we are the Data Processor and the client is the Data Controller). We must use such Personal Data only as instructed or authorized by the relevant customer and not for our (or anyone else's) purposes, except where expressly authorized by a written agreement with the relevant customer.	• **Maintain Confidentiality and Follow Contract.** You must always maintain the confidentiality and security of our customer's Personal Data in accordance with our contractual obligations to them. This includes only using the data as allowed by the contract. • **Contract Data Protection Language.** You must have appropriate data protection language in all agreements with customers. The Global Privacy Office has developed and will maintain appropriate language for use by the Company. Data protection language will provide customers with a right to request that we return or destroy any Personal Data we have collected from them, and we must abide by such requests. • **Questions about Customer Personal Data.** If we receive any questions or requests relating to Personal Data we use on behalf of our customers, we must inform the relevant customer and assist them, as appropriate under the circumstances, to respond to that request.

K. Vendor/Supplier Security Measures

#	Privacy Principle	What Does It Mean?	What Can You Do?
11	**Vendor/ Supplier Security Measures**	Where a service is being provided to us, including through vendors/suppliers, service providers or contractors (collectively "Vendor(s)") we engage or where we have subcontractors and there will be access to Personal Data by that Vendor or subcontractor, we must require such parties to agree to	• **Vendor and Subcontractor Data Protection Language.** You must have appropriate data protection language in all agreements with Vendors and subcontractors. The Global Privacy Office has developed and will maintain appropriate language for use by the Company. In the data protection language, we have the right to request that any Personal Data we provide to Vendors be returned or deleted. • **Third Party Risk Management ("TPRM") Process and Vetting of Vendors.** You should submit all new Vendors or expanded scope with an existing Vendor request through the Procurement and TPRM teams so that the Vendor can be vetted for all appropriate risk issues, including, without limitation privacy and security.

		appropriate data protection language.	

L. Direct Marketing Law Compliance

#	Privacy Principle	What Does It Mean?	What Can You Do?
12	**Direct Marketing Law Compliance**	We must adhere to all data protection laws that apply to our marketing efforts, including honoring all opt-out/unsubscribe requests as well as an individual's choices/preferences.	• **Honoring Choices and Preferences.** It is a best practice to provide an individual with choices and the ability to express preferences about how we communicate with them and for what purposes. Where we provide such choices, we must respect any preferences we receive from individuals. • **Providing and Honoring Opt-Out/Unsubscribe.** Where required by law, we must provide individuals with the ability to opt-out/unsubscribe from any and all communications we send, and we must honor such opt-out/unsubscribe requests. We recognize the Global Privacy Control signal (GPC) utilized by individuals in their website browsers and extensions. • **Opt-in Where Required.** Where required by law, we must obtain the required opt-in consent from individuals before sending them marketing communications, for example, by email or text. • **Use of Company Platforms, Apps, Processes and Procedures for Consent and Preference Management.** Where the Company has provided you with a platform, app, process or procedure for obtaining consent or preferences or managing such consent and/or preferences, you must use such tools as you have been directed. • **Marketing Department Involvement.** You must coordinate all marketing campaigns with your respective OpCo Marketing Department.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases,

applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 Exception Handling

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 Supporting Documents

- Artificial Intelligence ("AI") Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy

9 Document Information

Document Name	Personal Data Protection Policy
Issue Date	1 January 2024
Next Review Date	1 January 2025
Author(s)	Maureen Dry-Wasson
Maintainer	Christen Grapes
Owner	Maureen Dry-Wasson

10 Version History

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Nov 1, 2010	First Policy under name "Privacy and Personal Data Protection Policy"
2.0	Nov 1, 2011	Version 2 – annual review for updates
3.0	Jan 1, 2013	Version 3 – annual review for updates
4.0	Jan 1, 2014	Version 4 – annual review for updates
5.0	Jan 1, 2015	Version 5 – annual review for updates
6.0	June 1, 2016	Version 6 – Name of Policy changed to "Privacy and Personal Data Protection Policy" to "Employee Privacy Policy" and made other changes to adopt Global Privacy Principles
7.0	March 1, 2017	Version 7 – Updated definition of Personal Data and Sensitive Personal Data; added training and education language to enforcement section; other minor updates and changes
8.0	Nov. 18 2018	Annual review – updated logo
9.0	Jan. 1 2020	Used new template; changed name of Policy to "Personal Data Protection Policy"; included references to GDPR Compliance Policy and CASL Compliance Policy; changed Global Privacy Principles to chart format

10.0	Jan. 1, 2021	Annual review – Updated definition for Sensitive Personal Data; added more details regarding Data Subject rights requests and handling of government intelligence requests for Personal Data; Updates to Privacy Shield no longer being lawful transfer mechanism; clarified when to report privacy related incidents and when to send an email to Privacy Office; minor typos and wording changes
11.0	Jan. 1, 2022	Annual review – Added biometric data to the definition of Sensitive Personal Data for all individuals and clarified which financial data is Sensitive Personal Data for all individuals; added examples for minimum necessary information to the Relevant principle; added information regarding return or destruction of Customer Personal Data to Retain Only As Needed principle; added clarifications that reporting an incident means following the process in Section 2; minor typos and wording changes
12.0	Jan. 1, 2023	Annual review – minor wording changes and updates to reflect additional privacy laws in Virginia, Connecticut and Colorado.
13.0	Jan. 1, 2024	Annual review – Added additional explanation for incident reporting; added information security framework policies chart; updated for Data Privacy Framework; updates for China, Japan and other APAC countries; added provision related to TPRM process; minor wording changes
14.0	Jan. 1, 2025	Annual review – Changes to Incident Reporting and scope section consistent with changes made in all Information Security Program policies; added defined term of “Europe” for the EEA, UK and Switzerland and made appropriate changes throughout; added new section 5.2 regarding training since such training was already occurring; made updates to China in cross-border transfer section; added references to the new AI Center of Excellence; minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

GDPR Compliance Policy

Document ID:	AG-ISMS-POL-GDP
Version Number:	6.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This GDPR Compliance Policy (the "Policy") is part of the Information Security Policies Framework and describes the measures the Company employs to maintain compliance with GDPR. It applies in addition to the "Personal Data Protection Policy" which establishes the Company's baseline requirements for data protection globally.

Processing Personal Data is critical to the Company's business. For example, it is needed in order to:

- Provide services to customers;
- Promote services to prospective customers;
- Recruit Company Personnel as part of our business operations; and
- Carry out internal management and administration of the Company and its employees, including working with vendors.

As an organisation that processes Personal Data, the Company has a duty and obligation to uphold the rights and freedoms of Data Subjects. It is also critical for our business that our staff, customers and vendors are confident that their Personal Data is safe and that the Company will use it in accordance with applicable data protection laws.

This Policy is intended to provide a high-level overview of the measures required by the Company's GDPR Compliance Program. It does not detail the specifics of how those measures are implemented. Specific responsibilities, processes and guidance will be contained in documents referenced within this Policy.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, and any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section shall, for all purposes of this Policy, have the meanings specified as follows:

(1) "**Candidates**" means potential contractors, consultants and/or temporary workers that are, or may be, engaged by the Company so that the Company can provide their services to Company clients.

(2) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(3) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(4) "**Crime Data**" means Personal Data relating to criminal convictions and offences.

(5) "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

(6) "**European Sensitive Personal Data**" means information collected from or about individuals in Europe (collectively "Europe" for purposes of this Policy refers to the EEA countries, the UK, and Switzerland)) relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, as well as data concerning health or data concerning a person's sex life or sexual orientation. In some European member states, it may also include information about a person's criminal convictions.

(7) "**European Staff**" means Staff based in Europe.

(8) "**Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(9) "**GDPR**" means collectively, the European Union's Regulation (Europe) 2016/679 (General Data Protection Regulation) the UK Data Protection Act 2018 (UK GDPR) and the Swiss Federal Act on Data Protection (FADP). Where the context requires, "GDPR" will also refer to the member state laws which implement or supplement GDPR, as they apply.

(10) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time). For purposes of this Policy, Personal Data means any Personal Data subject to protection under GDPR.

(11) "**Rights Request**" means any form of request by a Data Subject made to the Company (in its capacity as data controller) seeking to exercise their rights as a Data Subject under GDPR, including without limitation rights of access, erasure and portability, or seeking to exercise similar rights within the scope of this Policy.

(12) "**Sensitive Personal Data**" means collectively European Sensitive Personal Data, any type of Personal Data that is considered "sensitive" data under applicable data protection law and for all individuals, regardless of applicable data protection law, includes health data, biometric data, genetic data, certain financial data, specifically, an individual's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, immigration and citizenship status and social security numbers or other national identification numbers and national identity documentation (such as passports).

(13) **Staff**" means collectively the employees, contractors, temporary workers, directors, consultants or other persons engaged to work for the Company. "Staff" does not refer to Candidates provided to Company clients.

(14) The terms, '**controller**', '**processing**', **'processing activity'**, '**processor**' and **'personal data breach**' have the meanings defined in GDPR.

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote location). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not, the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.12 DATA PROTECTION OFFICER (DPO)

A. Reasons for DPO Appointment

The Company shall appoint appropriate independent Data Protection Officers (DPO) for Europe, specifically for the UK, Germany, Switzerland and Belgium to oversee and advise on its GDPR Compliance Program. The primary purpose of the appointment is to ensure the Company has access to impartial, expert advice and the decision to appoint a DPO is not dependent on the Company being obliged to do so under GDPR. To ensure the independence of the DPO, they shall:

- Not be an employee of the Company;
- Have no other duties to the Company other than acting as DPO; and
- Not have a designated line manager or supervisor or otherwise be subject to any reporting lines.

B. DPO Appointment Process

When a DPO needs to be appointed:

- Potential candidates shall be recommended by the General Counsel EMEA Region, in consultation with the Global Privacy Officer; and
- The final candidate shall be selected and approved by the Allegis Group Data Protection Oversight Committee.

5.2 EMEA Privacy Incident Response Plan

The Company shall maintain a Privacy Incident Response Plan for the EMEA region under the Company's Global Security and Privacy Incident Response Policy in order to:

- Document the process for the Risk Team in EMEA to lead the handling of EMEA Privacy Incidents (including, but not limited to, Personal Data breaches);
- Provide the information and establish the resources needed for those processes to be carried out quickly and effectively;
- Establish a clear and effective procedure for all Staff to report Privacy Incidents to the Risk Team and document how all Staff are made aware of it; and
- Post the EMEA Region Privacy Incident Response Plan to a centralized location accessible by all appropriate Company Personnel who have a need to access it.

5.3 Data Subject Rights

A. Principles for Responding to Data Subject Rights Requests

The Company will:

- **Prompt and Professional –** act in accordance with law in addressing Data Subject Rights Requests and will promptly and professionally respond to them (or where appropriate, forward them to the appropriate controller or otherwise comply with any contractual obligations to the controller where Allegis is acting as a processor), observing the timeframes and requirements established by GDPR.
- **Balance Rights –** at all times, attempt to strike the correct balance between rights of different Data Subjects whose rights conflict in fulfilling a Data Subject Rights Request.
- **Consider Company Rights –** where necessary, consider its own rights to retain data and/or to keep it confidential to protect its own interests and the interests of its clients or other third parties and ensure, where relevant, that those reasons comply with guidance from the relevant data protection authority.
- **Provide Reasons –** should Allegis decline a Data Subject Rights Request (in whole or part) for any reason, it shall specify its reasons to the Data Subject in writing.

B. Handling of Data Subject Rights Requests – Responsible Parties

The Company has appointed the EMEA Risk Team to take the lead in handling and responding to Data Subject Rights Requests arising from the EMEA region, but performing this function requires the co-operation of all Staff. In particular:

- **Logging/Tracking –** All Rights Requests shall be logged and tracked in a centralized system.
- **Privacy Analyst Involvement –** The EMEA Risk Team will involve the appropriate Privacy Analyst(s) in any Data Subject Rights Request.
- **Staff Responsibilities –** When asked, all Staff must inform Data Subjects how they can submit Data Subject Rights Requests and promptly refer any Rights Requests that they receive themselves to the Risk Team. All Staff must promptly and fully co-operate with instructions from the Risk team in order for the Company to fulfil a Rights Request (including but not limited to instructions to provide or permanently delete the Personal Data the Data Subject Rights Request relates to).
- **Legal Assistance –** The Legal Team in EMEA will provide guidance to the Risk Team on the validity of Data Subject Rights Requests and the steps required to respond to them.
- **Information Technology Assistance –** The Information Technology architecture/infrastructure functions shall ensure all Company systems used to hold Personal Data can meet the System Technical Requirements below and shall

consider those requirements in the design stage of any new systems being developed or the requirements for any systems being procured. The Information Technology operations functions shall ensure they have procedures and resources in place to perform the system actions needed in the System Technical Requirements below on instruction by the Risk or Legal Teams.

C. Government Intelligence Data Requests. If you receive a request from a government or law enforcement for access to any Personal Data we hold for purposes of national security intelligence, you must report that immediately to the Global Privacy Office by reporting a Privacy Incident. The Global Privacy Office will handle all such requests as per the Company's Government Intelligence Data Request Policy and Procedures.

D. System Technical Requirements

To respond correctly and effectively to Data Subject Rights Requests, all Company systems used to hold Personal Data must allow the Company to:

- **Determine Systems –** Determine which Data Subjects that system holds data on, and what points of data are held on each Data Subject;
- **Locate Data in Systems –** Locate all the data within that system on a particular Data Subject (given enough information was provided to positively and uniquely identify that Data Subject);
- **Update or Remove Data –** Uniformly update or remove a particular data point(s) on a Data Subject on all records in the system;
- **Delete or Anonymise –** Either permanently delete any of the system's records on a Data Subject or anonymise those records (where anonymise means keeping the record itself in place but redacting the Personal Data within it so that it is no longer possible to identify the Data Subject that the record referred to); and
- **Export Data –** Export a copy of all the data on a Data Subject in an editable, human-readable format (either as one or as several documents).
  To the extent it is relevant to the system's intended purpose, Company systems used to hold Personal Data should, as far as possible, allow the Company to:
  - **Log of Sharing of Data –** Log which records have been shared with third parties (for example, which candidate profiles were sent to which clients);
  - **Source of Data-** Log the source of the data we have about the Data Subject (for example, how the Company came to have the Personal Data);
  - **Make Inaccessible –** Temporarily make a record inaccessible to system's users; and
  - **Automatic Decision Logic (where applicable) –** Provide a reasonable explanation of the logic the system uses to make automatic decisions (including profiling) with significant impact on the Data Subject and allow 'override' of such decisions with human intervention.

It is not necessary (but is preferred) for there to be a specific feature or functionality within the system to achieve the above requirements automatically, where possible. The ability of the system administrators to meet the requirements by manual intervention is also acceptable, provided there are sufficient resources in place. For example – if a system does not have a feature to export a machine-readable form, but it is possible for IT to create one by querying the system's database, this satisfies the requirement.

5.4 PRIVACY NOTICES

A. Contents and Drafting of Privacy Notices

The Company will maintain Privacy Notices as required under GDPR and ensure Data Subjects are provided with them and/or informed on how to access them.

The Legal Department in consultation with the Global Privacy Office is responsible for drafting Privacy Notices in a concise, transparent, intelligible and easily accessible way, using clear and plain language. Other departments and stakeholders may be consulted on the text, but the Legal Department has authority to determine and approve the final contents and how they will be structured. The Global Privacy Office will be responsible for final sign-off and publishing of Privacy Notices.

The Legal Department will also determine, in consultation with the Global Privacy Office, whether the Company will maintain multiple Privacy Notices for the EMEA region to account for:

- differences in applicable law between jurisdictions;
- distinct categories of Data Subjects whose Personal Data is processed for different purposes;
- variation in practise or business model between Company business units; or
- any other reason.

B. Publishing of Privacy Notices

All external facing Company websites must either include their own page(s) containing the applicable external Privacy Notice(s) (as content in the body of the page or as downloadable pdfs) or link to the corresponding pages on Allegis Group's primary external website. Such links and pages must be prominent and accessible to all users. Any Company based in Europe shall make its internal Privacy Notice available to all European Staff on its intranet site. The Privacy Notice to European Staff must be prominent and easily located.

C. Informing Data Subjects of How to Access Our Privacy Notices

The primary methods for informing external Data Subjects on how to access our Privacy Notices are:

- By a prominent link to it in all Company email footers; or
- By a prominent link to it on all webforms, portals, job advertisements, questionnaires or other systems or documents which invite Data Subjects to provide Personal Data to the Company.

For processing activities for which these methods would not be effective (for example, processing activities which do not involve the Data Subject being contacted by email or making use of the system or document referring them to the Privacy Notice), specific additional methods for informing external Data Subjects about the Privacy Notices should be established as part of the process for each relevant function(s) that carry out those processing activities.

European Staff will be informed on how to access their Staff Privacy Notice as part of their Company induction process.

5.5 DATA PROTECTION BY DESIGN AND BY DEFAULT

A. Privacy Impact Reviews and Data Protection Impact Assessments (DPIAs)

The Company's Policy is to assess risks to the privacy of Data Subjects before proceeding with significant changes to the ways it processes Personal Data such as new projects, new service lines, changes to our IT infrastructure and/or product portfolio, and engaging third party suppliers to process Personal Data on our behalf. The purposes of Privacy Impact Reviews are:

- To identify potential risks to the rights or freedoms of Data Subjects and/or to the security of processing by the Company;
- Suggest mitigations to address those risks;

- Ensure data protection is considered as part of the design and implementation of systems, services, products and business practices; and
- Determine if the risks require a formal Data Protection Impact Assessment (DPIA).

B. Company Policies – Data Protection Implications

Data Protection shall be considered in drafting all new and amended Company policies. Such policies should describe the data protection implications of the Policy and how the Policy addresses them. The nature of the data protection information required will depend upon the subject matter of the Policy, but should include as a minimum:

- The purpose(s) and lawful basis for the processing activities governed by it (if any);
- Which persons (by role or function rather than name) shall have access to the Personal Data involved; and
- Any specific measures required to mitigate the risk of harm to Data Subjects.

C. Commercial Contracts and Procurement – Data Protection Contract Provisions

The Global Privacy Office and Legal Teams shall provide guidelines to the Company's commercial and procurement functions on agreeable and compliant data protection conditions with clients and suppliers. Such guidance shall be periodically reviewed to be up-to-date with the Company's business lines and will include guidance on:

- Contracting on a controller-to-controller basis;
- Being engaged as a processor by a controller;
- Engaging a processor as a controller; and/or
- Engaging a sub-processor as a processor.

5.6 TRAINING AND AWARENESS

A. Training Programs

All Staff will receive mandatory general data protection training over an annual cycle. Auditable records of completion will be maintained to monitor attendance. Additional function-specific training will be provided for teams and departments which regularly process Sensitive Personal Data or whose functions otherwise present significant data protection risks. The content, mode of delivery and frequency of training programs will be regularly reviewed to monitor its effectiveness in providing sufficient guidance.

B. Privacy Liaisons

The Company may appoint Privacy Liaisons within departments who will be persons of sufficient authority and/or experience with specific data protection responsibilities or risks. Appointment as Privacy Liaison will be voluntary, except that where no suitable volunteer comes forward, the Company can require the Department's Manager (and/or their deputies) to fulfill this role. The Privacy Liaison will (in addition to their usual role):

- Promote best practise and champion the importance of secure data processing in the context of the day-to-day business of their department;
- Support their colleagues with data protection queries and concerns;
- Highlight needs for further training or guidance;
- Act as a focal point for addressing risks and implementing improvements to processes used by their teams; and
- Be the primary source of data protection updates or regulatory guidance within each department.

C. Written Guidance

Where the Company issues written guidance to Staff, it will ensure that such guidance is kept prominently available for as long it applies. For guidance applicable to all Staff for a Company, this will usually entail publishing the guidance on the applicable Company's intranet.

5.7 Information Security Policy Framework

The Company maintains a group-wide Information Security Policies Framework. One of the purposes of this Framework is to facilitate effective data protection by measures, such as:

- Applying appropriate technical security measures to the systems used to process Personal Data;
- Setting the information security standards and policies which Company Personnel and vendors of the Company are required to comply with;
- Monitoring Company systems for failures and attacks;
- Providing security incident reporting and response systems; and
- Requiring third party vendors of IT products or services to apply appropriate information security measures.

Further information on the Information Security Policies Framework is available by viewing all the policies within the Framework, which are available on the Company's intranet.

5.8 Data Handling by All Staff

The following are required in addition to adherence to the Company's Acceptable Use of Electronic Resources Policy:

A. Use of Designated Systems by All Functions

The Company expects all Staff to only process Personal Data using systems approved by the Company for the processing activity. Department Heads must ensure their teams have suitable systems for the processing activities they perform and guidance on how to correctly use those systems. They should raise any concerns by reporting such concerns as an incident under this Policy. As much as possible, Staff should avoid using their own manual or 'offline' methods such as:

- Using their own spreadsheets or other documents to keep lists of contacts, candidates or other Data Subjects;
- Saving Company records on desktops or in personal folders rather than in the designated system for those records;
- Saving copies of emails outside their mailboxes or other Company approved locations such as document management systems;
- Printing, copying, emailing or extracting material from a Company system, whether for reference or otherwise; or
- Unnecessarily emailing colleagues documents which are accessible on the designated company system.

B. Disposal of Manual Records

Although it should be kept to a minimum, the Company recognises that use of personal files, notes, working documents, print-outs, and/or hard copies ("Manual Records") may be necessary for teams or individual members of Staff to achieve their objectives and perform their work.

Where Staff have created Manual Records containing Personal Data, they must be disposed of as soon as possible when they are no longer needed. For example:

- Paper notes about a meeting or phone call should be destroyed once the relevant facts are recorded in the Company database;

- A spreadsheet used to decide which candidates to shortlist to a client for a vacancy should be disposed of once the shortlist is sent; and
- Print-outs must be disposed of once members of Staff have finished using them.

For the purpose of this section, 'disposing of' a record means:

- For computer files, permanently deleting (e.g. emptying the "recycle bin" on Windows PCs) all copies from all file locations (including your desktop, personal drive, any portable media, and any shared drives); and
- For paper records, disposing of the record as confidential waste according to the procedures in place in the location (which, in most locations will entail shredding the document, or placing the document in the secure waste bins provided).

C. Password Protection of Email Attachments

Accidently emailing Personal Data to the wrong recipients or accidently emailing more Personal Data than was intended form the most frequent causes of Personal Data breaches. For this reason, relevant documents should be password protected (so that the document cannot be opened without the password) before they are sent as email attachments if unintended disclosure of the document's contents presents any significant risk to any Data Subjects identified in that document. The Company takes a risk-based approach and does not require all email attachments containing Personal Data to be encrypted or password protected as this would be disproportionate and would significantly impact the effectiveness of our services and the likelihood of consistent data protection compliance. Passwords should be used when the document:

- **Significant Volume of Personal Data –** contains Personal Data on a significant number of Data Subjects (even if that data is not particularly sensitive or confidential);
- **Significant Confidential Nature of Sensitive Personal Data –** contains Personal Data which is significantly confidential or sensitive (even if that data only identifies a relatively small number of Data Subjects); or
- **Distribution to Large Number of Recipients –** contains Personal Data and will be distributed to a large number of people or otherwise used in a way that makes it more likely to be accidently disclosed.

Examples of documents that would require password protection are:

- Reports/spreadsheets containing information about a number of people (such as a list of all current contractors at a particular client);
- Status reports with detailed information on the performance or conduct of one or more people; and/or
- Copies of passports, medical reports or other sensitive documents.

Although care must always be taken to only send to the correct recipients, password protection is not required when sending:

- A CV (or small number of CVs) to a client contact;
- Invoices and timesheets; and/or
- Any document that is publicly available (e.g. material posted on our external website)

More specific guidance on particular documents and situations may be issued by department leaders.

Please note this Policy only describes requirements to password protect for data protection reasons. Documents may also need to be password protected for other reasons, such as confidentiality, even if they do not contain any personal data. In addition, you are encouraged to consider methods other than email for transmitting documents that need to be password-protected such as loading them to an encrypted thumb drive to mail to the recipient (and then

call the recipient to provide the password) or upload them to a secure FTP site where available (for example when sending files to a vendor, they may provide such an FTP portal).

D. Effective Password Protection

For Microsoft Office documents, the option to add password protection can be found on the application's main menu under File/Info/Protect Document>Encrypt with Password.
When sending emails with a password protected document(s):

- Use a password that is not obvious;
- Do not use the same password every time;
- Do not include the password in the same email as the document; and
- Where practical, communicate the password by a means other than email (to reduce the risk of sending both the password and the document to the same incorrect email address).

E. Other Electronic Communications

The rules in this section concerning email also apply equally to all methods of electronic communication.

5.9 DATA INVENTORY MANAGEMENT

A. Data Mapping

The Global Privacy Office shall conduct regular data mapping exercises to investigate the Company's data processing activities, handling of personal data and records retention practices. The specific goals shall be to:

- Document where we have European Personal Data stored;
- Re-evaluate our Records Retention Schedule and make adjustments where appropriate;
- Improve efficiencies around how we are storing records within and across departments and OpCos; and
- Give transparency to our collection, use and sharing of personal data so we can improve our privacy and information security efforts around that data.

The frequency and methodology of data mapping exercises shall be determined by the Global Privacy Office.

B. Processing Register as Controller

The information gathered from the data mapping exercise shall be used to form the records of processing activities (conducted as data controller) required under Article 30(1) of the GDPR. Where the processing activity involves the processing of Crime Data or Sensitive Personal Data requiring specific authorisation under European or European Member State Law, the register must include the following information (in addition to the information required under Article 30(1) of the GDPR):

- The legal provision by which processing is authorized by European or European Member State Law,
- How the processing satisfies Article 6 of the GDPR (lawfulness of processing), and
- Whether the personal data is retained and erased in accordance with this Policy and, if it is not, the reasons for not following this Policy.

C. Processing Register as Processor

Each Company that acts as a data processor on behalf of its clients shall maintain its record of processing activities (conducted as a data processor) required under Article 30(2) of the GDPR. The form of the record and the method for maintaining it shall be determined by the

applicable Company. Where appropriate, the record may be decentralised within the Company's commercial record for each client (the data controller).

D. Retention and Deletion

The Company has a Data Minimization Policy that includes a Records Retention Schedule as part of its global Information Security Policy Framework. The Records Retention Schedule(s) are issued to specify how long different record types are to be maintained before being deleted. The Privacy Office shall use the information obtained from data mapping and other sources to ensure that all record types are addressed by the Records Retention Schedule(s) and that the periods set for records containing Personal Data apply the principle of Storage Limitation, as more fully described in the Data Minimization Policy.

5.10 PROCESSING OF CRIME DATA

Under Article 10 of the GDPR, all processing by the Company of Personal Data relating to Crime Data must be authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

Any new proposed processing activity involving Crime Data must be risk assessed under the "Privacy Impact Reviews and Data Protection Impact Assessments" section of this Policy. Should the activity be approved following the impact review, the company shall:

- Document how the activity is authorised under European, European Member State or national law and ensure this is noted in the register of processing activities; and
- If appropriate or required by law, draft an appropriate Policy document governing the activity.

5.11 PROCESSING OF SENSITIVE PERSONAL DATA

The Company aims to minimise the amount of European Sensitive Personal Data (also known as the Special Categories as defined by Article 9 of the GDPR) it processes, but it may be necessary in certain circumstances, such as:

- Monitoring racial/ethnic origin, gender, and disabilities for equal opportunity monitoring or affirmative action programmes, if required by law;
- Where it is necessary to provide the Data Subject with a service;
- Drug/alcohol testing;
- Fitness-for-duty testing;
- Establishment, exercise or defence of legal claims;
- Absence monitoring and medical records of internal employees; and/or
- To comply with Health and Safety regulations.

Any new proposed processing activity involving European Sensitive Personal Data requires a risk assessment under the "Privacy Risk Assessments and Data Protection Impact Assessments" section of this Policy. Should the activity be approved, following the Risk Assessments, the company shall:

- Document how the activity complies with Article 9 of the GDPR;
- Where applicable, document how the activity is authorised under European or European Member State law and ensure this is noted in the register of processing activities; and
- If appropriate or required by law, draft an appropriate Policy document governing the activity.

Note that specific authorisation under European or European Member State law is not required (e.g. not required in addition to GDPR compliance) where European Sensitive Personal Data is processed:

- With the prior consent of the Data Subject;
- In the vital interest of the Data Subject (or of another natural person where the Data Subject is physically or legally incapable of giving consent); or
- For the establishment, exercise or defence of legal claims.

5.12 International Transfers of Personal Data

A. Company Policies Regarding International Transfers

As an international organisation with its world headquarters located in the United States that uses shared systems to serve multi-national clients and globally-mobile candidates, the Company often needs to transfer Personal Data internationally to conduct its business. Consequently, the Company's Policy on the international transfer of Personal Data outside the EEA is:

- **Maintain Appropriate Safeguards** – The Company will maintain Appropriate Safeguards (as defined in article 46 of the GDPR) to allow for Personal Data to be legitimately transferred to any Company within the Allegis Group family of companies worldwide (without the necessity to obtain express consent from Data Subjects on each occasion);
- **Reasonably Necessary** - The Company permits such internal transfers where they are reasonably necessary for operational, commercial or practical reasons; and
- **Compliance with this Policy** - All Companies in the Allegis Group family of companies processing such Personal Data must process it in accordance with this Policy (and the other relevant policies referenced within).

B. Appropriate Safeguards - Global Data Transfer Agreement

These practises, and the safeguards in place, will be outlined in all Privacy Notices. The intra-group safeguards currently in place are:

- **Global Data Transfer Agreement -** All Companies within the Allegis Group family of companies are bound by the Global Data Transfer Agreement, which incorporates the appropriate standard contractual clauses for the transfer of Personal Data to third country controllers and to third country processors.
- **EU-US Data Privacy Framework ("DPF"); UK Extension to the EU-US DPF and Swiss-US DPF (collectively referred to as "DPF").** These new frameworks replaced Privacy Shield. The frameworks were respectively developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for Personal Data transfers to the United States from Europe while ensuring data protection that is consistent with European law. We had maintained our Privacy Shield certification and have transitioned it to a DPF certification which means that transfers of Personal Data from Europe to the US are considered "adequate" under GDPR (an alternative to signing the Standard Contractual Clauses). To provide evidence of our certification to outside parties, provide this link: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000XZY0AAO&status=Active

C. Appropriate Safeguards – Vendor Agreements and Customer Agreements

When transferring Personal Data from Europe to vendors outside of Europe or when clients are transferring Personal Data from Europe to our Company located outside of Europe, we will maintain Appropriate Safeguards (as defined in article 46 of the GDPR) to allow for Personal Data to be legitimately transferred as necessary in such situations utilizing Standard Contractual Clauses or, where applicable, other transfer mechanisms recognized as adequate under applicable data protection law.

6 Enforcement

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 Exception Handling

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 Supporting Documents

- Acceptable Use of Electronic Resources Policy
- Data Minimization Policy
- Information Security Policy
- Personal Data Protection Policy
- Privacy Impact Review Procedures

9 Document Information

Document Name	GDPR Compliance Policy
Issue Date	1 January, 2025
Next Review Date	1 January, 2026
Author(s)	Steven Rhodes
Maintainer	Christen Grapes
Owner	Steven Rhodes

10 Version History

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	1 Jan 2020	First version issued
2.0	1 Jan 2021	Annual review – Updates for changes to Privacy Shield; minor typos and wording changes
3.0	1 Jan 2022	Annual review – updated definition of Sensitive Personal Data to match definition in Personal Data Protection Policy; added Global Privacy Office role in Privacy Notice review and posting; added language to International Transfer section regarding transfers to vendors and related to customers; minor typos and wording changes
4.0	1 Jan 2023	Annual review – updated definition of Sensitive Personal Data to match definition in Personal Data Protection Policy; added note about saving emails to document management systems as being an acceptable practice; added suggestions for ways to send Personal

		Data that needs to be password-protected other than email; minor typos and wording changes
5.0	1 Jan 2024	Annual review - Added additional explanation for incident reporting; added full ist of Information Security Framework policies; updated definitions to address UK GDPR; updated transfer section to address Data Privacy Framework; minor wording changes
6.0	1 Jan 2025	Annual review – Updated Incident Reporting and Scope sections consistent with minor changes made to all Information Security Program Framework policies; changed EU to Europe throughout; other minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Data Minimization Policy

Document ID:	AG-ISMS-POL-MIN
Version Number:	13.0
Issue Date:	01, January, 2025
Next Review:	01, January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

This Data Minimization Policy (the "Policy") is part of the Information Security Policies Framework and gives guidance on how the Company handles its Records.

The purpose of this Policy is to ensure that the Company's Records are collected, processed, stored, audited, protected, maintained and ultimately destroyed in a manner that meets legal, regulatory and contractual obligations.

The Company must retain Records for legal and commercial reasons and as part of good governance, but it is neither necessary, nor advisable, to retain all Records for longer than is necessary. There are several legal and regulatory requirements which establish minimum retention periods for certain types of Records. In addition, there are business reasons why we want to retain Records for a certain period to be able to defend claims or to effectively operate our business.

Data protection and privacy laws in many countries require that Personal Data, which many Records contain, must be kept for no longer than is necessary for the purposes for which the information was collected or for which it is further processed. Therefore, we must always consider whether there is an objective reason to keep Personal Data, in order to justify its retention.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- Company Personnel are expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(2) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's

information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(3) "**Data Subjects**" means the identified or identifiable person to whom Personal Data relates.

(4) "**Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(5) "**Litigation Hold Notice**" means a communication from the Company's legal department that informs you that Records you may have are relevant to current or anticipated litigation, an audit, a government investigation or other similar matter.

(6) **"Paper Inventory Handler**" means a person who is responsible for maintaining the system of record of offsite paper Records for a particular area of the Company. This person may be the same as the Records Handler within a given area.

(7) "**Personal Data**" any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(8) "**Records**" means documents and electronically stored information related to the Company's business activities, regardless of the medium or format of the information or its location. Records may contain Company information or third-party information, such as customer, vendor or business partner information. Records may or may not contain Personal Data.

(9) "**Records Handler**" means a person who handles and/or stores Records.

(10) "**Records Liaisons**" means employees the Company has appointed and trained who are points of contact throughout the Company responsible for providing advice and direction regarding adherence to this Policy by the Records Handlers.

(11) "**Repository**" means any system, equipment or facility (physical, electronic or otherwise) used for the storage, organization and/or retrieval of Records.

(12) "**Restricted Records**" means a Record which the Company needs to retain but may only process for a restricted set of reasons (the "**Restricted Purposes**").

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote location). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a default, follow this Policy or may provide their own Policy, as long as, such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not, the activities involving Company's informational assets are conducted from the Company's premises, conducted during working hours, or on Company-owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 PRIVACY BY DESIGN AND DEFAULT FOR RECORDS

A. Privacy by Design

When the Company is:

- Designing, developing, obtaining or modifying any Repository;
- Designing any process for the collection of Personal Data;
- Planning to collect or create a new type of Record; or
- Considering using a new application on an existing Repository

the Company must take into account this Policy, and other relevant Company policies, in developing its designs and Company Personnel must consult the Global Privacy Office where appropriate.

Resources to achieve Privacy by Design include, but are not limited to:

- **The Global Privacy Office and the Privacy and Protection Team ("PPT")** have been established to develop, monitor and enforce privacy policies, including this Policy.
- **The Data Protection Oversight Committee** has been set up to maintain supervision over privacy policies within the Company.
- **Training** in data protection regulation, law and practice has been provided to all relevant Company Personnel.
- **Liaisons** exist between the Privacy, Information Security and Information Systems (IS) functions to ensure continuity of objectives and the technical means to achieve them.
- **Privacy Policies** are designed to implement regulatory changes and additionally promote best practices in privacy within the Company.
- **Communications** are shared on privacy matters to update knowledge and awareness on privacy issues within the Company.

B. Privacy by Default

When the Company is:

- Conducting its daily business activities;
- Administering its current and historic business;
- Handling new or existing data; or
- Responding to requests or instructions from Data Subjects or data controllers

the Company must build good data handling practices into its habits, procedures and processes so that best privacy standards are maintained.

Steps to achieve this include, but are not limited to:

- **Restricted Access.** Access to Records (and the data within them) should, as far as practical, be restricted to Company Personnel who have an identified need for access.
- **Collection Purposes.** No Personal Data should be collected without at least one defined and reasonable purpose, and you must take adequate measures to prevent usage inconsistent with those purposes.
- **Retention Period.** Every Record type held by the Company must have a retention period defined within the Company's Records Retention Schedule.
- **Secure Repositories.** Repositories must be made as secure as reasonably possible, taking into account the business needs, available security measures and the risk (likelihood and severity) of a breach of security and ensuing harm to Data Subjects.
- **System Oversight.** Any information technology systems used in the collection, storage or processing of Records are subject to the oversight and approval of the Company's Information Security Office and must comply with any applicable security standards set by that Office.

5.2 Records Handlers and Records Liaisons

A. **Records Handlers.**

The Records Handler is responsible for the protection of any Records he/she/they handles including storage, retention and disposal of such Records.

B. **Records Liaisons/Managers.**

The Records Liaison is responsible for providing advice and direction regarding adherence to this Policy by the Records Handler within his/her/their respective area. This responsibility is in addition to the Records Liaison's customary full-time job duties. Records Liaisons should inform the Global Privacy Office of concerns or issues they discover regarding Records such as becoming aware that their assigned areas have access to Records which they do not require. Records Liaisons will complete any assigned data minimization training and provide assistance and cooperation to the Global Privacy Office to complete any data inventory, data minimization or records management projects, as needed. The Records Liaison is responsible for notifying the Global Privacy Office if he/she/they change roles with the Company and need to transition their Records Liaison duties to a new person by sending an email to the Global Privacy Office at privacyofficer@allegisgroup.com.

5.3 Storage Requirements and Litigation Hold Notices

A. Records Retention Schedule.

The Company creates and maintains Records Retention Schedules to provide appropriate retention times for all types of Records held within the Company. Each jurisdiction within which the Company is established may have its own specific retention requirements, often based on local law. If you believe you have a Record type that is not covered by the retention schedule, you should reach out to privacyofficer@allegisgroup.com for further guidance. If a Record type has no specific retention period, then the default for such Record types is that it should be kept for as long as there is business value and delete such Records as soon as they are no longer useful. Please ensure that you always refer to the appropriate schedule for your region/country, which can be found here.

B. Records Retention Time Periods.

The retention times specified in the Records Retention Schedule have a business justification and comply with legal, regulatory or contractual requirements. These time periods may be impacted for the situations outlined in D, E and F below.

C. Storage of Hard-Copy Records and Paper Inventory Handlers.

Where Records are to be retained in hard-copy, you must decide, in consultation with your Records Liaison, whether the Records will be kept on-site or off-site. Where Records are held on-site, you must ensure that the Records are properly and securely stored (for example, locked filing cabinets and/or rooms). Where physical Records are kept off-site, the Paper Inventory Handler should maintain a register of these Records as directed by the Company using an approved off-site storage vendor. The Records Liaison is responsible for notifying the Global Privacy Officer of the identity of the Paper Inventory Handler and of any changes related to the person filling this role by sending an email to the Global Privacy Office at privacyofficer@allegisgroup.com. The Paper Inventory Handler is responsible for completing any required data minimization training and for maintaining the Company's system of off-site paper Records for their area.

D. Obligations to Retain Records on Behalf of a Third Party.

If a client services agreement or other contractual obligation requires that Records be maintained for a period other than the periods of time set out in an applicable Records Retention Schedule, the retention period in the contract (whether longer or shorter than that in the Records Retention Schedule) will apply. Note that where the Company is holding Records as a "data processor" on behalf of a third party, that third party's reasonable documented instructions on which specific Records to retain, when to delete or return them and the means of deletion or return must be abided by, even if not specifically agreed in advance in the contract.

E. Litigation Hold Notices.

A Litigation Hold Notice is only authorized if sent from the Company's Legal Department. If you receive a Litigation Hold Notice:

- The Records you have that are relevant to the Litigation Hold Notice will be considered an exception to any stated destruction period in the Records Retention Schedule;
- You must cooperate with the Litigation Hold team to preserve and not delete, dispose, destroy or change those Records, including emails, until the Legal Department tells you that the Litigation Hold Notice has been removed; and
- Records containing Personal Data that would have been deleted if not for a Litigation Hold Notice shall be treated as Restricted Records (see section 5.4).

F. Data Subject Requests.

If an individual identified in the Record (a Data Subject) has made a valid Data Subject request under applicable data protection law related to their Personal Data (or part of it), for example, to access, correct, or delete, the relevant Personal Data shall be processed as necessary to address the Data Subject request by the deadline under applicable data protection law. The Global Privacy Office handles all Data Subject requests and therefore shall determine whether the request is valid and, if valid, confirm to the Company what Records and information must be, for example, accessed, corrected or deleted. If you receive a Data Subject request, you should immediately forward the request to privacyofficer@allegisgroup.com for further handling by the Global Privacy Office.

5.4 RESTRICTED RECORDS

A. What Are Restricted Records?

Restricted Records are those which must be kept under a higher standard of security than ordinarily applies. They include, but are not limited to Records:

- **Litigation Hold Notice:** which are being retained only because of a Litigation Hold Notice;
- **Objection by Data Subject:** for which an individual identified in the Record (Data Subject) has made a valid objection (as determined by the Global Privacy Office) to the use of the Record; and/or
- **Purpose No Longer Applies:** for which one or more of the Company's purposes for collecting the Record no longer applies, but that must be kept for statutory or other legal or regulatory purposes.

B. Purpose Restrictions.

Restricted Records must not be processed for any purpose other than their Restricted Purpose. When the Company is in possession of Restricted Records, we must take reasonable measures to prevent further processing. Those measures will depend on the nature of the Restricted Records and their Restricted Purpose but may, if appropriate, include:

- **User Access Restriction.** Restricting user access to the Record;
- **Redaction.** Redacting information from the Record which is not required for the Restricted purpose;
- **Marking Record Restricted.** Clearly marking the Record as Restricted, with sufficient information for any reader to understand the restriction; and/or
- **Storage Change.** Storing the Record securely outside the usual Repository for Records of that type.

5.5 DESTRUCTION OF RECORDS AND RETENTION IN ANONYMOUS FORM

A. **Destruction of Records.**

Records must be destroyed when they reach the end of their retention period, as determined under section 5.3. All physical Records disposed of under this Policy must be securely destroyed by a method which ensures the information is irrecoverable. For paper Records, you should dispose of them in the Company provided shredding bins if they contain any Personal Data or Company confidential information (unless local procedures have indicated that you can dispose of all paper Records in the Company provided shredding bins). Electronic Records may be considered destroyed if the information contained within the Record is ***permanently and irretrievably put beyond use***. The IS operations department responsible for maintaining the Repository shall determine the appropriate technical means to achieve this, taking account of any applicable standards defined by the Information Security Office.

B. **Retention in Anonymous Form**.

The Company may have a use or need for some Records which does not require those Records to personally identify any individual, for example, statistical analysis of historical data. Where this applies, the Record Retention schedules may permit the Records to be retained indefinitely provided they have been made anonymous. Records are only considered anonymous if:

- **No Identification.** The Record does not name, or otherwise provide the means to positively identify, any individual the information in the Record relates to; and
- **No Re-identification.** The Company has no means to "re-identify" those individuals, including by combining the Records with other information, whether that information is held by the Company or a third party.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), electronic resources such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 EXCEPTION HANDLING

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Personal Data Protection Policy
- Records Retention Schedule

9 DOCUMENT INFORMATION

Document Name	Data Minimization Policy
Issue Date	01, January 2025
Next Review Date	01, January 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Christen Grapes
Owner	Maureen Dry-Wasson

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Nov 1, 2011	First version issued as “Records Retention Policy”
2.0	Jan 1, 2013	Annual review
3.0	Jan 1, 2014	Annual review
4.0`	Jan 1, 2015	Annual review
5.0	June 1, 2016	Annual review
6.0	March 1, 2017	Annual review – updated definition of Sensitive Personal Data; added training and education language to enforcement section; minor typos and wording changes
7.0	Nov. 18, 2018	Annual review – updated logo

8.0	Jan. 1, 2020	Annual review – used new template; changed name of Policy to “Data Minimization Policy”; added provisions for compliance with GDPR (e.g., added Privacy by Design and by Default and data subject rights sections); changed “Records Managers” to “Records Liaisons”
9.0	Jan. 1, 2021	Annual review – addition of Paper Inventory Handler role; added more detailed definition regarding Records Liaison responsibilities; minor typos and wording changes
10.0	Jan. 1, 2022	Annual review – added reference to the new Privacy and Protection Team for their role with data minimization; minor typos and wording changes
11.0	Jan. 1, 2023	Annual review – Revised section on data subject rights to be broader than just deletion and provide other examples of data subject rights; minor typo corrections
12.0	Jan. 1, 2024	Annual review – Added additional explanation for incident reporting; added full ist of Information Security Framework policies; added explanation for how to handle Records with no retention period; minor wording changes
13.0	Jan. 1, 2025	Annual review – Minor changes to the Incident Response and Scope section consistent with changes made to all other Information Security Program Framework policies; clarified what it means to re-identify data in Paragraph 5.5B; other minor wording changes.

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

CASL Compliance Policy

Document ID:	AG-ISMS-POL-CSL
Version Number:	8.0
Issue Date:	01 January, 2025
Next Review:	01 January, 2026

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

1 CONTENTS

1 INTRODUCTION

The Company is committed to complying with the provisions of the Canadian Anti-Spam Legislation ("CASL"). This CASL Compliance Policy is part of the Information Security Policies Framework and outlines the Company's compliance program under CASL and defines what appropriate behavior is for you in complying with the rules set out in CASL.

CASL regulates the handling of commercial electronic messages ("CEMs"). CEM means any email or text message where one of its purposes is to promote the Company's services or events. Subject to limited exceptions, CASL requires that CEMs only be sent to recipients who have consented (through express or implied consent), unless a consent exemption applies. CEMs must also clearly identify the sender and allow the recipient to withdraw consent.

In addition, CASL prohibits fraudulent data collection, and alteration of transmission data, installation of a computer program, or use of a computer program to send messages, without express consent, and collecting Personal Data from a computer using a computer program or unauthorized access.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them. The Company needs your help in identifying those incidents and violations.

An incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Personal Data or other Company confidential information, interference with information technology operations, any violation or concern related to the subject matter of this Policy. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately.
- Company Personnel are expected to cooperate in the investigation.
- Retaliation towards those who report incidents and violations of this Policy in good faith or for cooperating in an investigation is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We", "our" or "Our" or "us" or "Us".

(2) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) and who have access to the Company's systems and information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

(3) "**Electronic Resources**" means any (a) information technology equipment, devices or related equipment (such as servers, computers, laptops, desk phones, mobile phones, tablet PCs (e.g., iPad), thumb drives or other storage devices or multi-function printer/copier/scanner/fax machines); (b) electronic key fobs/cards; (c) internet and internet connections; (d) intranets; (e) network file shares (such as the Q:, S:, T:, U: or O: drives); (f) file sharing sites (such as Team Sites, OneDrive and SharePoint); (g) databases; (h) online subscriptions and services (such as WebEx or LinkedIn Recruiter); (i) applications, whether cloud or on-premise (such as Office 365, voice mail or PeopleSoft, Salesforce ("Connected") or Bullhorn); (j) CCTV and any other similar resources of any kind each of which are (i) supplied by the Company to you for use for work-related purposes or (ii) not supplied by the Company to you, but are either: (a) used by you to connect to any Company network or (b) used in a way that affects the Company, whether intended or not.

(4) **"Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework (see the full list of policies in the last section of this Policy), including any supplements and/or procedures related to those policies.

(5) "**Personal Data**" means any information that relates to an identified or identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

4 SCOPE

The target audience of this Policy is Company Personnel. Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote location). Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site), may be subject to additional policies provided to the Company Personnel by that third party. Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may as a default follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises, conducted during work hours or on Company owned systems or equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 CASL COMPLIANCE PROGRAM

The following are in place to ensure the Company has an effective CASL compliance program:

A. Oversight for Compliance

The Company's Global Privacy Office is responsible for overall compliance of CASL. If you have any questions or concerns regarding the Company's CASL responsibilities, you should direct them to CASLcompliance@allegisgroup.com.

B. Use of Company's CEM Delivery System

If you are authorized to send CEMs on behalf of the Company, you must use the Company's CEM delivery system, which is subject to monitoring as explained in the Company's Workplace Monitoring Policy and allows the Company to maintain accurate records relating to the sending of CEMs and the tracking of unsubscribes.

C. Training

If you are authorized to send CEMs on behalf of the Company, you must complete the Company's CASL compliance training program and sign-off on completion.

D. CASL Compliance Rules

If you are authorized to send CEMs on behalf of the Company, you must comply with the CASL Compliance Rules set forth in Section 5.2.

E. Marketing Requirements

You must comply with the Direct Marketing Law Compliance Global Privacy Principle explained in more detail in the Company's Personal Data Protection Policy. As noted in that Policy, you must coordinate all marketing efforts with your OpCo Marketing Department. Local offices are not authorized to establish separate marketing campaigns or programs without first coordinating with their OpCo Marketing Department. For example, this means local offices are not authorized to send out email marketing campaigns or create accounts for the management of such campaigns (e.g., Constant Contact).

F. Complaint Handling

Any complaints related to CASL or anything in this CASL Policy should be immediately reported as an incident under Section 2.

5.2 CASL COMPLIANCE RULES

In addition to otherwise complying with the Company's Acceptable Use of Electronic Resources Policy, if you use the Company's Electronic Resources, including using third party services via the Electronic Resources to do any of the following, you must follow these rules to comply with this CASL Compliance Policy:

- **Follow Company Procedures for Sending CEMs.** When transmitting, distributing or delivering CEMs (even if it is a single CEM), you must follow the Company's procedures for sending CEMs.
- **No Misleading Representations.** You must not transmit, distribute or deliver any message (whether or not it is a CEM) with false or misleading representations, whether in the sender information, subject matter of an electronic message or in a locator (including a URL). For example, the message cannot contain false or misleading information in the subject line or false or misleading content in the message.
- **No Downloading/Installing Applications to Violate CASL.** You must not download or install any applications onto the computer system that would, or could be used to, violate CASL.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company-provided subscription based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 Exception Handling

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department. Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 Supporting Documents

- Acceptable Use of Electronic Resources Policy
- Personal Data Protection Policy
- Workplace Monitoring Policy

9 Document Information

Document Name	CASL Compliance Policy
Issue Date	01 January 2025
Next Review Date	01 January 2026
Author(s)	Maureen Dry-Wasson
Maintainer	Christen Grapes
Owner	Maureen Dry-Wasson

10 Version History

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	March 1, 2017	First version issued as “CASL Policy”
2.0	Nov 18, 2018	Annual review – updated logo
3.0	Jan. 1, 2020	Annual review – used new template; changed name of Policy to “CASL Compliance Policy”
4.0	Jan. 1, 2021	Annual review – updated person responsible for CASL compliance to Sr. Privacy Specialist – Global; minor wording changes and typos
5.0	Jan. 1, 2022	Annual review – updated title for person responsible for CASL compliance due to title change and added new Canadian based member of Global Privacy Office; minor typos and wording changes
6.0	Jan. 1, 2023	Annual review – updated person responsible for CASL to the Privacy Staff Attorney with Global Sr. Privacy Specialist for additional support
7.0	Jan. 1, 2024	Annual review – Added additional explanation for incident reporting; updated definition of Electronic Resources added full list of Information

		Security Framework policies; removed specific titles and just referenced Global Privacy Office for compliance with CASL
8.0	Jan, 1, 2025	Annual review – Minor changes to the Incident Response and Scope section consistent with changes made to all other Information Security Program Framework policies

11 INFORMATION SECURITY FRAMEWORK POLICIES

- Acceptable Use of Electronic Resources Policy
- Artificial Intelligence (“AI”) Policy
- Bring Your Own Device (“BYOD”) Policy
- CASL Compliance Policy
- Data Minimization Policy
- GDPR Compliance Policy
- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy