Information Security Management Framework

Information Security Policy

Document ID - AG-ISMS-POL-01

Effective Date: 1 January 2018

Next Review Date: 1 January 2019

Table of Contents

1 Introduction

The Information Security Policy (the "Policy") contains important rules covering information security and protecting the confidentiality, integrity, and availability of information assets within the Company.

The Policy establishes safeguards and controls to protect the Company's informational assets from loss and from unauthorized access, modification, destruction, or disclosure.

This Policy describes the organization of the Information Security Office, mandates the roles within the Information Security Office, and documents the operations of the group in executing this Policy. This Policy also explains when you must get the approval of the Information Security Office.

This Policy outlines the controls that must be in place to protect the Company's informational assets when those assets are created, received, transmitted, copied, accessed, modified, or destroyed. This includes rules around storage of data and encryption of data.

1.1 Document Context

This document is an integral part of Company's Information Security Management Framework (ISMF). The ISMF provides structure to the development and maintenance of security controls in order to actively manage information security threats and risks targeting the organization's information assets.

1.2 Related Policies

The following documents are related and relevant to this document. Copies of them are available on the Company's intranet.

Ref#	Reference Document Name	Document ID	Version	Owner/ Author
1.	Information Security Policy	AG-ISMS-POL-01	7.0	Information Security Office
2.	Information Classification Policy	AG-ISMS-POL-02	7.0	Information Security Office
3.	Acceptable Use Policy	AG-ISMS-POL-03	7.0	Information Security Office
4.	Online Privacy Policy	AG-ISMS-POL-04	16.03.01	Information Security Office
5.	Social Media Policy	AG-ISMS-POL-05	7.0	Information Security Office
6.	Employee Privacy Policy	AG-ISMS-POL-06	7.0	Information Security Office
7.	Records Retention Policy	AG-ISMS-POL-07	6.0	Information Security Office
8.	Bring Your Own Device Policy	AG-ISMS-POL-08	1.0	Information Security Office

2 Intended Audience

The target audience of this document is Allegis Group, Inc. and its subsidiaries worldwide (referred to as the "Company"), all 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 (for example payroll providers, benefits providers, auditors, lawyers) and who have access to the Company's systems and information under contract (collectively referred to as "Company Personnel", "You" or "you" or "Your" or "your").

3 Scope

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 or on Company owned 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.

4 Enforcement

This Policy is important to the Company, and it intends to provide you with additional training and/or education to you to assist you in complying with it. However, where appropriate, and where additional training and/or education is not sufficient, in the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access or use Electronic Resources 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.

5 Incident Reporting

It is important to the Company that it is aware of violations of this Policy so that it can appropriately address them, and the Company needs your help in identifying those violations. With regards to violations of this Policy:

- All violations of this Policy must be reported immediately.
- If you report violations of this Policy then you will be expected to cooperate in the investigation, however you will not be subject to reprisal or retaliation solely as a consequence of such good faith reporting or involvement.
- Retaliation is a very serious violation of this Policy and must be reported immediately.

You must report violations of this Policy as follows:

- If you are an employee, to your immediate supervisor or department head, and if you are a non-employee, to your Company contact person; **and**
- Online at https://infosec.allegisgroup.com/ **or**
- By telephone at +1-866-483-5411

6 Organization of Information Security

6.1 Management Commitment

6.1.1 The Company's management is committed to establishing a secure culture to protect you from risk, and to support the values of the organization in achieving excellence.

6.1.2 The Information Security Office takes responsibility for security in authorizing, supporting and executing on the Information Security Management Framework (ISMF).

6.2 Security Organization

6.2.1 One of the responsibilities of the Information Security Office is to seek to protect the interests of the Company against security risks. The Information Security Office regularly reviews risk to balance security controls with business needs.

6.2.2 To take responsibility for security, the Company has also appointed a Director of the Information Security, with direct responsibility for information security, the Information Security Management Framework, and the security of the Company's informational assets.

6.2.3 The Director of Information Security has appointed a member of the Information Security Office to manage governance and compliance for the policies within the Information Security Management Framework, with responsibility for auditing compliance with the policies and the underlying standards and processes of the Information Security Management Framework.

6.2.4 The Information Security Office will also include personnel who will execute the roles required by the Information Security Management Framework and its underlying processes. The Information Security Office will assure that these personnel have the required competencies, by means of suitable education, training, or experience, to execute their roles.

7 Controls

7.1 Technology Ownership and Use

7.1.1 Authorization for system access

(a) Your access to Company systems must be authorized through the assignment of an individual user account by the IS Department (with delegated authority

from the CIO).

(b) If you are a part of the Company's IS Department, you will take measures to protect data, including encryption, authorization and backups, to the standards set by the Information Security Office.

7.2 User Responsibilities

7.2.1 You must take appropriate measures to protect Company assets, including any information assets, whether those assets are in hard copy or electronic form.

7.2.2 Please see additional user requirements in the Company's Acceptable Use Policy, which is referenced in Section 1.2 above.

7.3 Approval Requirements

7.3.1 Before Electronic Resources, as defined by the Acceptable use Policy, can be supported and/or Company information is stored on them, the Electronic Resources must be properly approved and must be on the approved Electronic Resources register, which includes personal devices. The CIO is accountable for this approval process.

7.3.2 Security acceptance testing programs and related criteria must be established for new information systems and software, upgrades, and new versions. The Information Security Office must approve all programs and criteria. No system or software will be implemented or changed without either passing testing or being granted a formal exception by the Information Security Office.

7.3.3 The Company's IS Department will maintain a formal change management process. The Director of the Information Security or his/her designee, will be an approver of changes based on the risk and classification of the information involved and, when required, no change will be made without their approval.

(a) When the Director of Information Security or his/her designee, finds significant changes involving information with data privacy or data security legal compliance, the Information Security Office will be required as an approver of the change before any changes are made. The Information Security Office will audit the change for compliance and reject not compliant changes.

7.4 Removable Media/Mobile Devices

7.4.1 You are responsible for protecting all mobile, Company owned Electronic Resources, such as smartphones, laptops, USB drives and other removable media.

7.4.2 You must not connect personal removable media, such as CDs or DVDs, or devices, such as USB drives, to any Company network, and you must not use them to store Restricted or Highly Confidential information unless approved by the Information Security Office.

7.4.3 If you use removable media for the transportation of client confidential material, or Confidential, Highly Confidential, or Restricted Company information, you are required to use removable media that is encrypted using a Company approved encryption method. You may only store Public information on unencrypted or approved removable media. Additional requirements and guidance are set out in the Encryption section of this Policy.

7.4.4 You must protect approved removable media and portable devices at all times, including not leaving them unattended in public or other insecure areas (trains, cars etc.). You must also be aware of the environment around you to protect against the risk of unauthorized viewing of information or the attempted theft of the physical asset.

7.4.5 The Information Security Office may, at their discretion, grant network access to you for your use of personal devices but only after evaluating the risk the access presents and the mitigating controls that must be in place to control that risk. Please see the Company's Bring Your Own Device Policy for additional information regarding the use of personal devices referenced in Section 1.2.

7.5 Rogue Devices

7.5.1 Any device attached to the Company's network without permission will be considered a "Rogue Device". You must report any Rogue Devices to the Information Security Office, and the Information Security Office will immediately remove them from the network.

7.6 Information Classification and Handling

7.6.1 Information Labelling Standard

(a) Information is classified and may be labelled to establish a level of sensitivity around that information in accordance with the Information Classification Policy referenced in Section 1.2. This also assists in defining the controls required to protect information.

(b) During its lifecycle, the classification of information may change to become more or less sensitive. Information will be monitored to ensure it has the correct level of classification/controls attached.

7.6.2 Handling of Information

(a) The handling of information will be governed by its classification as covered by the Information Classification Policy. If you need clarification regarding the protection of information, you should contact the Information Security Office.

(b) Assets capable of storing, computing, processing, or communicating information will be reviewed by the Information Security Office and certified for the controls required to meet the requirements for each level of Information Classification.

(c) Information of each classification level will only be stored, computed, processed, or communicated on assets certified at or above that level of classification.

7.6.3 Destruction of Information

(a) You must destroy information in accordance with the Company's Records Retention Policy referenced in Section 1.2 above.

(b) The destruction of electronic media containing Company or third party information must only be carried out by the approved contractors appointed by the Director of Information Security and completed to the standards of the Information Security Office. The IS Department will assist with tools certified by the Information Security Office to meet the standards. The Information Security Office will audit contractors and tools for compliance with the policies and standards.

7.6.4 Malicious Software

(a) The introduction of malicious software to Company systems can have a serious impact on the confidentiality, integrity and availability of information. The Company has implemented industry leading technology to protect the organization from malicious software. However, you must still be vigilant in protecting systems from such software (for example, taking caution if receiving a suspicious email or having access to an unapproved storage device).

(b) You must report any instances of malicious software found on a Company asset to the Information Security Office. The Information Security Office will assess the risk of malicious software versus known vulnerabilities and escalate the response as appropriate.

(c) All software must be approved and listed on the Application Service Catalogue maintained by the Company's Enterprise Architecture team prior to being installed on any Company asset. The Information Security Office must be approvers on all software being added to the Application Service Catalogue.

(d) You are not permitted to download or install any software application onto the Company's network or Company owned devices, without the prior permission of the Director of Information Security for enterprise implementations or exception approval from the Information Security Office for individual users or instances.

7.7 Physical Security

7.7.1 Access to the Organization's Premises

(a) Access to any Company premises is for authorized Company Personnel only through the allocation of either an identity card or visitors pass. Any person authorized via a visitors pass must be accompanied by Company Personnel when moving around the office apart from in client areas such as client meeting room facilities.

(b) You must carry your Company-issued ID and/or other required identity at all times while on the premises and present them on request.

(c) Access to the building is recorded for security purposes through CCTV and access management systems.

7.7.2 Secure Areas

(a) You should assess the risk of breach or unauthorized access and sharing before performing work on the Company's information. When appropriate or required, you must perform the work in secure areas that keep the information from visual, audible, or electronic access to the information.

(b) Procedures will be documented for working in secure areas and enforced at all times in those secure areas. All those with access to the secure areas will be trained in these procedures.

7.7.3 Secure Area Access

(a) 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 room, power rooms, and project areas. These areas are labelled as such and advice is available from the Information Security Office as to how to get authorization for these areas.

(b) You may not attempt to gain access to these areas without authorization, even when you are accompanied by an authorized person.

(c) All access to secured areas must be logged and all logs must be reviewed at least monthly.

7.8 Encryption

7.8.1 Encryption will be used to protect the confidentiality, integrity/authenticity, non-repudiation, and authentication of information where appropriate based on risk and the classification of the data according to the Information Classification Policy.

7.8.2 Company information shall never be encrypted without the ability of the Information Security Office to decrypt the data. All use of encryption must be approved by the Information Security Office prior to use.

7.8.3 The Information Security Office will maintain a technical standard 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.

7.8.4 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, to whom the Information Security Office formally approves, oversees, guides and audits. All activity involving encryption keys shall be logged and audited.

7.9 Application Security

7.9.1 Secure engineering principles and rules will be developed and documented 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.

7.9.2 The Company will supervise the activity of outsourced development and the Information Security Office will monitor and audit this activity.

7.10 Monitoring

7.10.1 Company systems and facilities equipment are provided as a business tool. The Company retains the right to monitor all systems and physical areas of the business to protect the Company and Company Personnel and to ensure the appropriate use of the Company resources and information assets in compliance with privacy law and in accordance with the Acceptable Use Policy referenced in Section 1.2.

7.10.2 Systems have been 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.

7.10.3 Monitoring will be conducted of, but is not limited to, CCTV, email, Internet, laptops and desktop PCs when connected to any Company networks or systems.

7.10.4 Access to monitoring is controlled and limited to trained and designated administrators to ensure an acceptable level of confidentiality and privacy is achieved. If you have any concerns, you should raise them with the Information Security Office.

7.10.5 The exact purposes for which monitoring may be conducted and the parameters of such monitoring may depend from country to country to ensure such activities comply with applicable law. For more information on the monitoring activities of the Company, please read the Acceptable Use Policy. Inappropriate use detected through monitoring will be dealt with in accordance with the Company's usual HR processes and procedures relating to disciplinary matters, including as set out in the Employee Handbook.

7.11 Security Incident Management Guidelines

7.11.1 Security Incident Response Process (SIRP)

(a) To ensure an effective and appropriate response to security incidents, in particular, any lost items of removable media, organization owned or approved personal devices holding Company data, the Company has established a documented process to deal with incidents and you are responsible for reporting incidents in accordance with the Security Incident Response Process (SIRP).

(b) You must report all security incidents to the Information Security Office as soon as possible as set forth in Section 5 above.

(c) All security incidents must be evaluated and managed by the Information Security Office using the Security Incident Response Process.

(d) All notifications to third-parties regarding security incidents and/or potential data breaches must be approved by the Information Security Office.

8 Compliance

8.1 Data Protection and Privacy

You are responsible for data protection compliance with the guidance of the Information Security Office. You are responsible for ensuring the Company meets its requirements under the local law when processing personal data as set out in the Employee Privacy Policy referenced in Section 1.2.
If you have concerns relating to data protection violations, you must report those concerns as set forth in Section 5.

8.2 Copyright Law

You must comply with all applicable copyright Law. If you have any concerns regarding material and your ability to use it properly under copyright law, you should contact your Group General Counsel.

8.3 Export Restrictions

You must comply with all export restrictions around data, software, or hardware for all legal jurisdictions where business is conducted. You should consult with the Information Security Office if you need advice or guidance.

9 Auditing

The Information Security Office will enforce compliance with this Policy by performing audits, reviewing the causes of all significant security incidents, and assessing solutions prior to implementation or significant change. If non-compliance is found, the Information Security Office will document the event and require a corrective action plan.

10 Definitions

Unless otherwise defined in this Policy, all terms shall have the definition given to them under the ISO 27000 policies at:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435.

11 Exception Management

If the Company determines that it has a compelling need to do so, the Company may have requirements to circumvent defined security controls set forth in this Policy.

Exceptions can be requested by contacting the Service Desk at +1-866-483-5411. Such exceptions must be escalated to and cleared by the Information Security Office in order to ensure any additional controls are put in place to mitigate risk and any residual risk is accepted by the business.

12 Comments to Policy

If you have any questions or comments about this Policy or have suggestions to improve it, please send your comments to InfoSecOffice@allegisgroup.com.

13 Revision History

Ver No.	Effective Date	Author(s) Name	Revision Description
1	November 1, 2010	Maureen Dry-Wasson and Scott Henderson	N/A
2	November 1, 2011	Maureen Dry-Wasson and Scott Henderson	Version 2
3	January 1, 2013	Maureen Dry-Wasson and Dana Pickett	Version 3
4	January 1, 2014	Maureen Dry-Wasson and Dana Pickett	Version 4
5	January 1, 2015	Maureen Dry-Wasson and Dana Pickett	Version 5
6	June 1, 2016	Maureen Dry-Wasson and Dana Pickett	Version 6
7	March 1, 2017	Maureen Dry-Wasson and Andrew Sheppard	Version 7 – added training and education language to enforcement section; minor typos and wording changes

14 Governance and Policy Review Management

The Information Security Office will be responsible for any changes to this Policy. The Company's Information Security Policies will be reviewed on an annual basis to ensure that it remains appropriate to the needs of our organization. In addition to the pre-defined review, the Information Security Policy will continuously evolve to meet changing internal and external requirements, which may include:

- Changes to Company's business and IT environment or tolerance to risk
- Changes to regulatory requirements
- Changes to contractual requirements, and
- Changes to adapt to emerging risks & threats

Information Security Management Framework

Acceptable Use Policy

Document ID – AG-ISMS-POL-03

Effective Date: 1 January 2018

Next Review Date: 1 January 2019

Table of Contents

1 Introduction

This Acceptable Use Policy (the "Policy") sets out important rules governing the use of Electronic Resources, online services, the Internet, 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 network or affect the Company in any way, whether intentional or not.

Electronic Resources means desktops, laptops and related computer equipment, e-mail, intranets, file-sharing (such as SharePoint), or network file shares such as the S:, T: and U: drives, telephones, smartphones and other mobile phones, tablet PCs (such as iPads), , fax machines, copiers, multi-function devices , scanners, CCTV, electronic key fobs/cards and voice-mail which are either:

(a) supplied by the Company to you for use for work-related purposes; or

(b) not supplied by the Company to you but either they are used by you to connect to any Company network or their use by you affects the Company in any way, whether intentional or not.

(collectively "Electronic Resources").

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.

This policy also outlines the circumstances in which the Company will monitor by automatic means the use of Electronic Resources and the circumstances in which the Company may investigate activities that are flagged by monitoring tools as suspicious.

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 you. "Personal Data" means any information that relates to an individual such that it can identify them, including, without limitation, name, phone numbers, email addresses, national ID number, job history, banking information, and results of background checks.

1.1 Document Context

This document is an integral part of the Company's Information Security Management Framework (ISMF). The ISMF provides structure to the development and maintenance of security controls in order to actively manage information security threats and risks targeting the organization's information assets.

1.2 Related Policies

The following documents are related and relevant to this document. Copies of them are available on the Company's intranet.

Ref#	Reference Document Name	Document ID	Version	Owner/ Author
1.	Information Security Policy	AG-ISMS-POL-01	7.0	Information Security Office
2.	Information Classification Policy	AG-ISMS-POL-02	7.0	Information Security Office
3.	Online Privacy Policy	AG-ISMS-POL-04	16.03.01	Information Security Office
4.	Social Media Policy	AG-ISMS-POL-05	7.0	Information Security Office
5.	Employee Privacy Policy	AG-ISMS-POL-06	7.0	Information Security Office
6.	Records Retention Policy	AG-ISMS-POL-07	6.0	Information Security Office
7.	Bring Your Own Device Policy	AG-ISMS-POL-08	1.0	Information Security Office

2 Intended Audience

The target audience of this document is Allegis Group, Inc. and its subsidiaries worldwide (referred to as the "Company"), all 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 (for example payroll providers, benefits providers, auditors, lawyers) and who have access to the Company's systems and information under contract (referred to as "Company Personnel", "You" or "you" or "Your" or "your").

3 Scope

This Policy applies whether or not the activities involving the Electronic Resources are conducted from the Company's premises.

This policy establishes a minimum level of standards, with the option for 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.

4 Enforcement

This Policy is important to the Company, and it intends to provide you with additional training and/or education to you to assist you in complying with it. However, where appropriate, and where additional training and/or education is not sufficient, in the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access or use Electronic Resources 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.

5 Incident Reporting

It is important to the Company that it is aware of violations of this Policy so that it can appropriately address them, and the Company needs your help in identifying those violations. With regards to violations of this Policy:

- All violations of this Policy must be reported immediately.
- If you report violations of this Policy then you will be expected to cooperate in the investigation; however, you will not be subject to reprisal or retaliation solely as a consequence of such reporting or involvement.
- Retaliation is a very serious violation of this Policy and must be reported immediately.

You should report violations of this Policy as follows:

- To your immediate supervisor, department head or Company contact for non-employees; **and**

- Online at https://infosec.allegisgroup.com/ **or**

☐ By telephone at +1-866-483-5411

6 Controls

6.1 Principles Regarding Use of Electronic Resources

6.1.1 Only authorized users must have access to Electronic Resources.

6.1.2 When using Electronic Resources, you must always comply with any applicable laws and regulations, this Policy and the related policies set forth in Section 1.2. This includes, without limitation, protecting Personal Data in compliance with applicable data protection and/or information security laws and the Employee Privacy Policy.

6.1.3 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.

6.1.4 You must protect t all information (including Restricted, Highly Confidential and Confidential information, as defined in the Company's Information Classification Policy) owned by the Company and its licensees (for example, proprietary code) while such information is in the Company's custody.

6.1.5 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.

6.2 Unacceptable Uses of Electronic Resources

When using Electronic Resources, you must **not**:

6.2.1 Use Electronic Resources in a way that is abusive, obscene, discriminatory, racist or harassing.

6.2.2 Export software, technical information, encryption software or technology in violation of international or regional export control laws.

6.2.3 Engage in any activity which is illegal under any other applicable law.

6.2.4 Disclose or share 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, and as appropriate given the volume and sensitivity of the information, the Director of Information Security, or the appropriate business head has approved the disclosure.

6.2.5 Cause legal liability for the Company or damage the Company's brand or reputation or cause damage, distress, annoyance or any other form of harm to others.

6.2.6 Do anything to disrupt, damage, impair, interrupt, slow down or affect the functionality of the Electronic Resources, including any computer hardware or software, beyond your normal use.

6.2.7 Knowingly upload, transmit or post 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.

6.2.8 Use social networks or other websites in violation of their posted terms and conditions, such as by scraping contact information through automated means.

6.2.9 Advertise or offer to sell or buy any goods and services for any business purpose, unless specifically permitted to do so by your manager.

6.2.10 Impersonate another person or entity or create a false identity for the purpose of misleading another person.

6.2.11 Do anything that would interfere with another user's ability to use the Internet.

6.2.12 Send, upload, post or otherwise make available, or procure the sending of, any unsolicited or unauthorized advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes" or any duplicative or unsolicited messages.

6.2.13 Download, copy and/or distribute 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.

6.2.14 Install any software onto Electronic Resources without prior authorization from the Information Security Office.

6.2.15 Make 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.

6.2.16 Make 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.

6.2.17 Make or circulate commercial, religious or political statements or solicitations or promote businesses unrelated to the Company.

6.2.18 Connect any device to the Company's wired network without approval from the Information Security Office.

6.2.19 Conduct business activities or transmit 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 is considered secured and meets the standards).

6.2.20 Share Electronic Resources with family, friends and other third parties.

6.3 Use of Electronic Mail- Additional Provisions

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

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

6.3.3 You should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .exe). If you suspect that you have received a virus, you should report it to the Service Desk immediately to appropriately assess and assist in the remediation of the potential virus. The Service Desk will escalate if need be and the opening of a security incident may be required (see Section 5 for how to report).

6.3.4 In addition to the Unacceptable Uses of Electronic Resources outlined in Section 6.2, with regards to your use of e-mail, you must not:

a. Contribute to system congestion by sending or forwarding trivial messages (such as chain mail, junk mail, cartoons or jokes) or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them.

b. Agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained.

c. Send messages from another Company Personnel's computer or under an assumed name unless specifically authorized by the Information Security Office.

d. Use the Company's systems to send Sensitive Personal Data via e-mail or the Internet, or by other means of external communication which are not known to be secure.

i. Sensitive Personal Data includes "Sensitive EU Personal Data" which includes information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and

the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, 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. In addition, Sensitive Personal Data includes financial Personal Data about an individual, such as their bank account or payment card details and social security numbers and national identity documentation (such as passports) (collectively this information plus the Sensitive EU Personal Data is referred to as "Sensitive Personal Data")..

e. Access the Company's email from any device or use a connection method that is not provided by the Company or approved by the Information Security Office. Please see the Company's Bring Your Own Device ("BYOD") Policy for more information about using a personal device to access Company e-mail.
f. Engage in unauthorized use, or forging, of e-mail header information.
g. Solicit e-mail for any other e-mail address other than your own with the intent to harass or to collect replies.

6.3.5 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.

6.3.6 If you receive a wrongly-delivered e-mail, you must notify the sender, but you must not respond to SPAM or phishing e-mails.

6.3.7 You must not send 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 consent is required, without approval of the Information Security Office. The Information Security Office will only approve such email activity after verification that the email would not be considered SPAM and would not violate anti-SPAM laws (i.e. CAN-SPAM, CASL, e-Privacy Directive, etc.) for the legal jurisdictions involved.

6.4 Use of the Internet and Social Media- Additional Provisions

6.4.1 The Company recognizes the benefits and the opportunities presented by the Internet and social media sites. However, we must also ensure that your use of the Internet, social media and the Electronic Resources generally does not (i) jeopardize our confidential information or our intellectual property rights or (ii) risk putting the Company in breach of our legal, regulatory and contractual obligations.

6.4.2 Misuses of the Internet can, in certain circumstances, constitute a criminal offense. You are prohibited from accessing websites, web-directories or similar sources hosting or containing unlawful, obscene, immoral, derogatory, abusive, offensive 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.

6.4.3 Access to the Internet is restricted, and website access (including personal use of social media) is monitored and filtered in accordance with this Policy and applicable laws.

6.4.4 If you are contacted for comments about the Company, its products or the business for publication anywhere, including in any social media outlet, you are required to direct any and all inquiries to the Company's Marketing Department and you may not respond without written approval.

6.4.5 Access to social media, including, but not limited to, LinkedIn, Facebook, Twitter, Instagram, YouTube, or blogs using the Electronic Resources must be in accordance with all of the policies listed in Section 1.2, including without limitation the Allegis Group Social Media Policy.

6.5 Use of Real-time Conferencing and Instant Messaging ("IM") – Additional Provisions

6.5.1 Instant messaging communications and real-time conference sessions may not be secure and can be recorded. Sensitive Personal Data and/or Company confidential information must not be transmitted via such services unless security and confidentiality can be ensured.

6.5.2 The conditions described under section 6.9 concerning content that is marked "private" also apply to instant messages.

6.6 Use of External or Cloud Services

6.6.1 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).

6.6.2 The Information Security Office will audit these vendors at least once a year for compliance with the Company's security and privacy requirements and will assign each vendor a qualified level of information classification for the service.

6.6.3 You may only use cloud services on the approved list. Only information with a classification level at or below the qualified level of the service may be stored on the cloud service.

6.6.4 You must report as a security incident (see Section 5) 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.

6.7 Use of Electronic Resources for Payment Card Transactions

6.7.1 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.

6.8 Security, Accounts and Passwords for Electronic Resources

6.8.1 For further information on your obligations in relation to information security, refer to the Company's Information Security Policy.

6.8.2 You must change your account password at least every three months. 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. You should protect any Electronic Resources in accordance with the Information Security Policy and/or as is otherwise appropriate.

6.8.3 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. The Information Security Office can provide advice to you on creating and using good passwords.

6.8.4 Creation of new passwords and resetting of passwords will be a tightly controlled activity and must be performed to the standards of the Information Security Office. You must not implement any automated password creation or reset solutions without the review and approval of the Information Security Office.

6.8.5 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.

6.8.6 If you communicate passwords or other secret authentication information, you must do so securely according to the standards of the Information Security Office.

6.8.7 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 must be encrypted using a solution approved by the Information Security Office and in compliance with the Information Security Policy.

6.8.8 You must not download or install software from external sources without prior authorization from the Director of the Information Security. The Information Security Office uses best efforts to ensure that computers issued to you are equipped with virus protection software. All incoming files and data should always be checked by virus protection software. If you believe your computer does not possess virus protection software, you must alert the Information Security Office immediately.

6.8.9 You must not attempt to gain access to restricted areas of the Company's network, or to any password-protected information, unless you are specifically authorized. Any attempts to disrupt the network will be treated as a security incident, and responded to using the Security Incident Response Process. 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.

6.9 Monitoring Use of Electronic Resources (All Locations Other Than EEA)

6.9.1 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 in situations involving personal use. 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.

6.9.2 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 purpose, and regardless of whether any conditions or limitations on monitoring in the " Monitoring Use of Electronic Resources (Inside the EU)" subsection below are satisfied.

6.9.3 The Company's ability to conduct investigations in its discretion is not limited by this policy.

6.10 Monitoring Use of Electronic Resources (Inside the EEA)

6.10.1 This monitoring section is an exception to Section 6.9 that applies to any Company Personnel working inside the jurisdiction of the European Union or its member states. Other jurisdiction must also be granted this exception by the Information Security Office where appropriate.

6.10.2 You should be aware that any message, file, data, document, facsimile, telephone conversation, social media post or instant message communication, or any other kind of information or communication transmitted to or from, received or printed from, or created, stored or recorded on the Electronic Resources are presumed to be business-related and may be monitored by the Company in accordance with this Policy and applicable laws.

6.10.3 The Company will conduct automated monitoring of the Electronic Resources through automated tools such as anti-malware software, website filtering and e-mail SPAM filtering.

6.10.4 The purpose of this automated monitoring is to protect the interests of the Company, you and other Company Personnel, and the Company's customers and business partners by encouraging the positive behavior of the Company Personnel when they use Electronic Resources and investigating negative behaviors when it is necessary to do this. Without limiting the ability of the Company to monitor the Electronic Resources for additional purposes permitted by applicable laws, the Company may monitor the Electronic Resources for any of the following purposes:

- System and network security including in particular the security of the Electronic Resources and their use in accordance with this policy.
- Proof of business transactions and archiving.

- Coaching, training and evaluation of staff.
- Protection of the Company's confidential information.
- Other legitimate business purposes as permitted under applicable laws.

6.10.5 The automated monitoring activities may include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings (collectively, "Communications") and other uses of the systems as well as other network monitoring technologies, with the exception of content that is clearly marked by you as "private". If a Communication is not adequately marked, there is a risk that it will be opened and read by the Company. The Company will cease reading the Communication when the reader becomes aware that the Communication is private.

6.10.6 The Company's monitoring activities are generally continuous and ongoing. However:

- Monitoring activities will always be proportionate, for legitimate purposes and as required or permitted by applicable laws; and
- Before undertaking any monitoring activities, the Company will consider your reasonable expectations of privacy and assess whether there are any less privacy invasive options.

6.10.7 You must clearly identify private e-mails and messages by adding the term "private" in the e-mail or message's subject line and/or storing those e-mails/messages in a separate folder named "private". You may also create and store non-business related documents in a separate folder that is clearly marked "private" in the disk space named "my documents".

6.10.8 Where the Company must access content that is clearly identifiable as being private, it will do so only after informing the employee concerned, unless there is a particular risk or threat for the Company, or the Company has obtained a court order authorizing it do so.

7 Employee Separation Management

7.1.1 You must return all Electronic Resources that belong to the Company upon any separation of your employment or engagement with the Company.

7.1.2 The Company will disconnect you from all Electronic Resources, including, without limitation access to the Company's e-mail and the Company's networks, intranet, Software as a Solution or other Company-paid subscription services (for example Salesforce.com) and file shares upon separation or your employment or engagement with the Company.

8 Investigations

8.1.1 The Company reserves the right to carry out investigations, retrieve the contents of e-mails, messages, postings, files or check searches which have been made on the Internet for purposes including:

a. to monitor whether the use of the Electronic Resources or the Internet or social media is legitimate and in accordance with this Policy.
b. to find lost e-mails, messages, postings, files or to retrieve e-mails, messages, postings, files lost due to computer failure.
c. to assist in the investigation of wrongful acts, including assisting law enforcement agencies.
d. to comply with any legal obligation to which the Company is subject.

8.1.2 Such investigations will be made within the limits described in this Policy, and in accordance with applicable laws.

9 Definitions

Unless otherwise defined in this Policy, all terms shall have the definition given to them under the ISO 27000 policies at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435.

10 Exception Management

If the Company determines that it has a compelling need to do so, the Company may have requirements to circumvent defined security controls set forth in this Policy.

You can request an exception by contacting the Company's IS Service Desk at +1-866-483-5411. Such exceptions must be escalated to and cleared by the Information Security Office in order to ensure any additional controls are put in place to mitigate risk and any residual risk is accepted by the business.

11 Comments to Policy

If you have any questions or comments about this Policy or have suggestions to improve it, please send your comments to InfoSecOffice@allegisgroup.com.

12 Revision History

Ver No.	Effective Date	Author(s) Name	Revision Description
1	November 1, 2010	Maureen Dry-Wasson and Scott Henderson	N/A
2	November 1, 2011	Maureen Dry-Wasson and Scott Henderson	Version 2
3	January 1, 2013	Maureen Dry-Wasson and Dana Pickett	Version 3
4	January 1, 2014	Maureen Dry-Wasson and Dana Pickett	Version 4
5	January 1, 2015	Maureen Dry-Wasson and Dana Pickett	Version 5
6	June 1, 2016	Maureen Dry-Wasson and Dana Pickett	Version 6 – Name of Policy changed from Electronic Resources Policy to Acceptable Use Policy
7	January 1, 2017	Maureen Dry-Wasson and Andrew Sheppard	Version 7 – Updated definition of Electronic Resources and Sensitive Personal Data; added training and education language to enforcement section; minor typos and wording changes

13 Governance and Policy Review Management

The Information Security Office will be responsible for any changes to this Policy, and any changes shall be subject to the approval of the Company General Counsels. This Policy will be reviewed on an annual basis to ensure that it remains appropriate to the needs of our organization. In addition to the pre-defined review, the Policy will continuously evolve to meet changing internal and external requirements, which may include:

- Changes to the Company's business and IT environment or tolerance to risk
- Changes to regulatory requirements
- Changes to contractual requirements, and
- Changes to adapt to emerging risks & threats

Information Security Management Framework

Social Media Policy

Document ID - AG-ISMS-POL-05

Effective Date: 1 January 2018

Next Review Date: 1 January 2019

Table of Contents

1 Introduction

Allegis Group welcomes the growing use of Internet, mobile, and other social media networks such as Facebook, LinkedIn, Twitter, blogs and wikis and recognizes that they provide 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.

To minimize these risks, avoid loss of productivity and ensure that our IS resources and communications systems are used only for appropriate business purposes, we have created this Social Media Policy (the "Policy"), which deals with the use of all forms of Social Media by you to ensure compliance with the Company's Information Security Management Framework as well as any of the Company's legal obligations related to the use of Social Media.

This Policy also includes important information about the types of monitoring and surveillance activities the Company undertakes and the circumstances in which such activities may occur.

1.1 Document Context

This document is an integral part of the Company's Information Security Management Framework (ISMF). The ISMF provides structure to the development and maintenance of security controls in order to actively manage information security threats and risks targeting the organization's information assets.

1.2 Related Policies

The following documents are related and relevant to this document. Copies of them are available on the Company's intranet.

Ref#	Reference Document Name	Version No.	Owner/ Author
1.	Online Privacy Policy	7.0	Information Security Office
2.	Acceptable Use Policy	7.0	Information Security Office
3.	Information Security Policy	16.03.01	Information Security Office
4.	Employee Privacy Policy	7.0	Information Security Office
5.	Information Classification Policy	7.0	Information Security Office
6.	Records Retention Policy	6.0	Information Security Office
7.	Bring Your Own Device Policy	1.0	Information Security Office

2 Intended Audience

The target audience of this document is Allegis Group, Inc. and its subsidiaries worldwide (referred to as the "Company"), all 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 (for example payroll providers, benefits providers, auditors, lawyers) and who have access to the Company's systems and information under contract (referred to as "Company Personnel", "You" or "you" or "Your" or "your").

3 Scope

This policy establishes a minimum level of standards, with the option for 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. The scope of this Policy includes but is not limited to the following (collectively defined as "Social Media"):

Types of Social Media:

- Interactive social networking web sites (including but not limited to Facebook, Vine, LinkedIn, Snapchat, Tumblr, Reddit, Blab, Vine, Pinterest, and Instagram).
- Listservs or mailing lists; audio or video-sharing websites (such as YouTube and Flickr).
- Virtual worlds (such as Second Life); wikis; file-sharing applications; blogs or microblogs (such as Twitter).
- Internal social intranets or networks; text-messaging or "same-timing" using either instant-messaging software, cell phones, apps (such as GroupMe) or other mobile devices; and Company maintained sites (such as Yammer).

Uses of Social Media

- Both business and personal use of Social Media, regardless of how, where and when it's accessed.
- Services delivered directly to a customer of the Company, either at the customer's facility or remotely.
- Multiple-Use Accounts used to perform Company activities (see Section 6.2).

4 Enforcement

This Policy is important to the Company, and it intends to provide you with additional training and/or education to you to assist you in complying with it. However, where appropriate, and where additional training and/or education is not sufficient, in the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Social Media sites 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.

5 Incident Reporting

It is important to the Company that it is aware of violations of this Policy so that it can appropriately address them, and the Company needs your help in identifying those violations. With regards to violations of this Policy:

- All violations of this Policy must be reported immediately.
- If you report violations of this Policy then you will be expected to cooperate in the investigation; however, you will not be subject to reprisal or retaliation solely as a consequence of such good faith reporting or involvement.
-
- Retaliation is a very serious violation of this Policy and must be reported immediately.

You must report violations of this Policy as follows:

- If you are an employee, to your immediate supervisor or department head, and if you are a non-employee, to your Company contact person; **and**

- Online at https://infosec.allegisgroup.com/ **or**

☐ By telephone at +1-866-483-5411

6 Controls

6.1 Acceptable/Unacceptable Uses of Social Media

6.1.1 If you see or become aware of any negative posts on Social Media that could potentially harm the reputation of the Company, you must immediately report it to the leaders of the Marketing/Communications Department who will work with other departments (e.g., HR, Legal) as necessary to determine appropriate next steps.

6.1.2 You must use Social Media responsibly by exercising common sense, writing knowledgeably, and striving to be accurate and professional.

6.1.3 You must ensure that your privacy settings accurately reflect your intentions.

6.1.4 If you endorse Company products or services, you must disclose your relationship to the Company.

6.1.5 You must take the necessary precautions to prevent identity theft as that could jeopardize the Company's assets/resources. Some examples of precautions are:

a. Provide only basic information on Social Media
b. 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.

6.1.6 You must 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.

6.1.7 You must not misrepresent your identity or your ability to speak on behalf of the Company.

6.1.8 You must clearly indicate in your postings that it is your own/personal views and not the

Company's, unless you have been authorized to speak on behalf of the Company.

6.1.9 You must not post content that could be considered offensive, discriminatory, defamatory, harassing, insulting, violent or obscene.

6.1.10 Your activities on Social Media must not breach other Company policies (including without limitation those policies referred to in Section 1.2).

6.1.11 Your activities on Social Media must not violate any laws or regulations.

6.1.12 You must not directly or indirectly, disclose Company confidential information (including without limitation business strategies and goals, financial information and information about clients and candidates).

6.1.13 You must not attempt to gain unauthorized or unlawful access to someone else's Social Media account.

6.1.14 You must not request or require an applicant or Company Personnel to disclose their personal Social Media log-in credentials or reject an applicant or discipline or terminate Company Personnel for failure to do so, except as permitted by applicable law.

6.1.15 You must not use Social Media to discriminate against or exclude potential applicants or other Company Personnel.

6.1.16 Your activities must not violate the agreements that the Company has in place with its customers, service providers, or suppliers.

6.1.17 You must not plagiarize information, and all information must be properly attributed to the relevant sources.

6.1.18 You must not circulate chain letters or other spam to others.

6.2 Multi-Use Accounts

6.2.1 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 (such as LinkedIn, Twitter 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 (such Social Media accounts are referred to as a "Multi-Use Account"). 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.

6.2.2 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 should acknowledge and position the Company in accordance with the Company's brand and strategic marketing standards, which are managed by the Marketing departments.

6.2.3 If you are posting/publishing thought leadership that was created with or by the Company, the post/publish must clearly acknowledge an association to the Company.

6.2.4 You must enter into the appropriate database for your Operating Company (for example the any Company "CRM", or Client Relationship Management system, like Salesforce.com or the any Company "ATS", or Applicant Tracking System, like RWS or Connected) 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.

6.3 Company Social Media Accounts

6.3.1 A "Company Social Media Account" means any Social Media account that is used exclusively for business purposes to interact with any of the Company's current or potential contractors, candidates, clients, customers, vendors, or suppliers, 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.

6.3.2 For all Company Social Media Accounts, you must:

a. 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's IS Web & Creative Team.
b. Not create or operate any Company Social Media Accounts without prior authorization from the leaders of the Company's Marketing/Communications Department.
c. Provide any log-in credential information to the Company's IS Web & Creative Team and protect the log-in credential information as Restricted information under the Company's Information Classification Policy.
d. Follow any guidelines issued by your Operating Company regarding the creation and maintenance of Company Social Media Accounts and attend any required training.

7 Social Media Monitoring

7.1.1 The Company may monitor Social Media to validate compliance with this Policy.

7.1.2 The monitoring will be limited to the concerns listed in this Policy, namely to minimize the identified risks presented by the use of Social Media.

7.1.3 Monitoring the use of Social Media will preferably not take place at an individual level, unless misconduct is suspected. For further information regarding the Company's monitoring activities, please see the Acceptable Use Policy.

7.1.4 Personal information alleging misconduct under this Policy will be discussed with you and may be added to your personnel file.

8 Employee Separation Management

Upon any separation from employment or change in role, as applicable:

8.1.1 You must update your Social Media profile to accurately reflect your involvement with the Company.

8.1.2 Company Social Media Account users must close or transition the account to appropriate Company Personnel.

8.1.3 You must cease using any Multi-Use Accounts for the purpose of Company business.

9 Definitions

Unless otherwise defined in this Policy, all terms shall have the definition given to them under the ISO 2700 policies at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435.

10 Exception Management

If the Company determines that it has a compelling need to do so, the Company may have requirements to circumvent defined security controls set forth in this Policy. Such exceptions must be escalated to and cleared by the Information Security Office in order to ensure any additional controls are put in place to mitigate risk and any residual risk is accepted by the business.

11 Comments to Policy

If you have any questions or comments about this Policy or have suggestions to improve it, please send your comments to InfoSecOffice@allegisgroup.com.

12 Revision History

Ver No.	Effective Date	Author(s) Name	Revision Description
1	November 1, 2010	Maureen Dry-Wasson and Scott Henderson	N/A
2	November 1, 2011	Maureen Dry-Wasson and Scott Henderson	Version 2
3	January 1, 2013	Maureen Dry-Wasson and Dana Pickett	Version 3
4	January 1, 2014	Maureen Dry-Wasson and Dana Pickett	Version 4
5	January 1, 2015	Maureen Dry-Wasson and Dana Pickett	Version 5
6	June 1, 2016	Maureen Dry-Wasson and Dana Pickett	Version 6
7	March 1, 2017	Maureen Dry-Wasson and Andrew Sheppard	Version 7 – 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

13 Governance and Policy Review Management

The Information Security Office will be responsible for any changes to this Policy. The Company's Information Security Policies will be reviewed on an annual basis to ensure that it remains appropriate to the needs of our organization. In addition to the pre-defined review, the Information Security Policy will continuously evolve to meet changing internal and external requirements, which may include:

- Changes to Company's business and IT environment or tolerance to risk
- Changes to regulatory requirements
- Changes to contractual requirements, and
- Changes to adapt to emerging risks & threats

Information Security Management Framework

Employee Privacy Policy

Document ID - AG-ISMS-POL-06

Effective Date: 1 January 2018

Next Review Date: 1 January 2019

Table of Contents

1 Introduction

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 Employee Privacy Policy ("Policy"), which was formerly known as the Privacy and Personal Data Protection Policy, that requires you to ensure that the Personal Data we collect and use is handled in accordance with applicable data protection laws. "Personal Data" means any information that relates to an identifiable individual; an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as, name, phone numbers, email addresses, national ID (or other identification) number, job history, banking information, online identifier (like an IP address), health information, the results of background checks or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual. This may include, for example, characteristics that are unique to an individual, like a person's height, age category, regional origin or details about their profession or job function. The Company processes the Personal Data of employees (internal employees and employees we place with clients), interns, temporary employees, customers and vendors (including past, present and prospective individuals) and has a responsibility to ensure that it uses such Personal Data in accordance with all applicable laws.

1.1 Document Context

This document is an integral part of Allegis Group's Information Security Management Framework (ISMF). The ISMF provides structure to the development and maintenance of security controls in order to actively manage information security threats and risks targeting the organization's information assets.

1.2 Related Policies

The following documents are related and relevant to this document. Copies of them are available on the Company's intranet.

Ref#	Reference Document Name	Version No.	Owner/ Author
1.	Online Privacy Policy	7.0	Information Security Office
2.	Acceptable Use Policy	7.0	Information Security Office
3.	Information Security Policy	16.03.01	Information Security Office
4.	Social Media Policy	7.0	Information Security Office
5.	Information Classification Policy	7.0	Information Security Office
6.	Records Retention Policy	6.0	Information Security Office
7.	Bring Your Own Device Policy	1.0	Information Security Office

2 Intended Audience

The target audience of this document is Allegis Group, Inc. and its subsidiaries worldwide

(referred to as the “Company” or “we”), all 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 (for example payroll providers, benefits providers, auditors, lawyers) and who have access to the Company’s systems and information under contract and handle Personal Data (referred to as “Company Personnel”, “You” or “you” or “Your” or “your”).

3 Scope

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

(a) provide services to customers;

(b) promote services to prospective customers; and

(c) 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 will be covered by applicable data protection laws. It is critical that our 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.

This policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Council.

4 Enforcement

This Policy is important to the Company, and it intends to provide you with additional training and/or education to you to assist you in complying with it. However, where appropriate, and where additional training and/or education is not sufficient, in the event you violate this Policy, any one or all of the following further actions might be undertaken:

- 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.

5 Incident Reporting

It is important to the Company that it is aware of violations of this Policy so that it can appropriately address them, and the Company needs your help in identifying those violations. With regards to violations of this Policy:

- All violations of this Policy must be reported immediately.
- If you report violations of this Policy then you will be expected to cooperate in the investigation; however, you will not be subject to reprisal or retaliation solely as a consequence of such good faith reporting or involvement.

- Retaliation is a very serious violation of this Policy and must be reported immediately.

You must report violations of this Policy as follows:

- If you are an employee, to your immediate supervisor or department head, and if you are a non-employee, to your Company contact person; and

- Online at https://infosec.allegisgroup.com/ **or**
- By telephone at +1-866-483-5411

6 Controls - Global Privacy Principles

6.1 Ensure transparency by being open, honest and fair when using Personal Data.

6.1.1 Understanding the principle

a. Being open, honest and fair in the way we use and share Personal Data is an important step to demonstrate good data protection practices.

b. Individuals should be properly notified about who we are, what Personal Data we collect and why, and how we use and share their Personal Data.

6.1.2 Practical steps

a. Privacy notices must be provided to individuals, if possible at the time of collection of that information (e.g. in customer-facing documents such as application forms or on our websites) or as soon as practicable after that.

b. If third parties provide Personal Data to us, we should check that they have provided suitable privacy notices to the individuals concerned to explain that we will be handling their Personal Data.

c. We will provide a privacy notice to our employees, including our contract employees, where we collect and use Personal Data about them.

d. All contracts should include suitable wording, where applicable, notifying individuals of how we will use their Personal Data and explaining data protection requirements.

6.2 Use Personal Data only for specified and lawful purposes

6.2.1 Understanding the principle

a. We must only collect Personal Data for the purposes which are identified to an individual at the time of collection (or, where this is not possible, which are subsequently notified to them within a reasonable time) and which are permitted by law.

b. We must identify and publicize the purposes for which Personal Data will be processed in privacy notices and contracts.

c. If required by law, we must seek individuals' consent for the collection, use or disclosure of their Personal Data – this may be the case, for example, when collecting and using individuals' Sensitive Personal Data (see Principle 6.9 for further information).

6.2.2 Practical Steps

a. When collecting Personal Data from individuals, we must ensure that the privacy notice made available to those individuals contains all of the purposes for which the Personal Data may be used.
b. When collecting information, we must never collect Personal Data in a way that is unlawful or where we have no legitimate basis for using that Personal Data.
c. When collecting Sensitive Personal Data, we must ensure that we have obtained an individual's explicit consent.

6.3 Keep Personal Data accurate, complete and up-to-date to ensure data quality.

6.3.1 Understanding the principle

a. Processing inaccurate information can be harmful to individuals and to us.
b. We must actively encourage individuals to inform us when their Personal Data changes.

6.3.2 Practice steps

a. We must manually or by automated reminders, actively encourage employees, including contract employees, to update their Personal Data.
b. We must regularly encourage all customers and vendors to update their Personal Data. This might be done, for example, by inviting them to notify us of any changes in their Personal Data when we are communicating with them.
c. When we learn of any changes to Personal Data that individuals are not able to change themselves, we should be sure that the appropriate changes are made to ensure accuracy.

6.4 Collect only relevant Personal Data

6.4.1 Understanding the principle

a. We must only collect Personal Data for purposes that have been specified to the individual and ensure that the Personal Data we collect is not excessive.
b. We must not collect Personal Data which is irrelevant to the purposes for which it is sought.

6.4.2 Practical steps

a. When collecting Personal Data from individuals, we must ensure that we do not collect data which is outside of the scope of that set out in the privacy notice provided to those individuals.
b. We must guard against collecting excessive amounts of Personal Data from individuals. We must not collect more information than is necessary to fulfill specific business needs that have been communicated to the individual.

6.5 Retain Personal Data only for as long as it is necessary.

6.5.1 Understanding the principle

a. Any Personal Data relating to individuals should only be kept where there is a

business or legal need to do so and it should not be retained simply because it might come in useful one day without any clear view of when or why.

6.5.2 Practical steps

a. You should comply with our Records Retention Policy, which covers these practical steps and others in further detail.
b. Statutes or regulations may require that certain Personal Data be retained for a specified length of time, and it may also be prudent to keep certain Personal Data for a specific period so that we are able to defend properly any legal claims or manage an on-going business relationship, all of which is considered in the periods of time set forth in the Records Retention Policy..
c. If a customer requires us in a written contract to maintain Personal Data, we will maintain such Personal Data according to the customer's requirements.
d. Records containing Personal Data must not be kept indefinitely and should always be deleted and destroyed once they have become obsolete or when the Personal Data is no longer required.

6.6 Respect and honor the rights of individuals

6.6.1 Understanding the principle

a. We must reply to questions, complaints and requests concerning our processing of Personal Data in a reasonable period of time and to the extent reasonably possible in accordance with law. In many jurisdictions, individuals have the right to access Personal Data held about them (in both electronic and paper form), and we must honor such requests that are made to us in a prompt and efficient manner.
b. We will also comply with other data protection rights including:
    i. Individuals may object to our use of their Personal Data for direct marketing or for any purposes. Individuals may also express marketing preferences and we must respect them.
    ii. Individuals may ask us to change the information that we hold on them, in particular because they consider our information to be inaccurate or out-of-date.
    iii. Individuals may ask us to confirm that no decision taken by us is based solely on the processing of their Personal Data by automatic means for the purpose of evaluating matters relating to them, for example, their creditworthiness or employability.
    iv. Individuals may ask us to delete information held about them.

6.6.2 Practical steps

a. You must always coordinate marketing efforts with your Marketing Department to ensure that we are adhering to applicable law related to marketing campaigns.
b. Where we receive a request from an individual exercising the right to access their Personal Data, we must follow the steps set out in our Subject Access Request Procedure. Our procedure provides a timeline of events to ensure that valid requests are processed in accordance with applicable law.
c. Where you need assistance in responding to a request from an individual exercising any data protection right, you should contact your Group General Counsel.

6.7 Protect Personal Data by taking appropriate security measures.

6.7.1 Understanding the principle

a. All Personal Data must be kept secure.

b. We must apply appropriate technical and organizational measures to protect individuals' Personal Data from unauthorized or unlawful processing or disclosure and from accidental loss, destruction, or damage.

6.7.2 Practical steps

a. We must monitor the level of security applied to each set of information, taking into account current standards and practices.

b. When considering what level of security we must apply to a set of information, 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 to be protected.

c. When engaging a third party to collect, store or use Personal Data on our behalf, we must impost strict contractual obligations on them dealing with the privacy and security of that information.

d. In particular, we must observe the requirements set out in the Information Security Policy and related policies mentioned in Section 1.2.

6.8 Ensure adequate protection for international transfers of Personal Data

6.8.1 Understanding the principle

a. Some territories do not allow transfers of Personal Data to other territories unless an adequate level of data protection exists for the Personal Data on its receipt.

b. For example, international transfers of Personal Data outside of the European Economic Area ("EEA") are not allowed without appropriate steps being taken to ensure the adequate protection of the transferred data. Such steps include our entering into standard contractual terms with the proposed recipient of the transferred data.

6.8.2 Practical steps

a. We must not transfer any Personal Data internationally (including outside of the EEA) without appropriate steps being taken, such as standard contractual clauses, to protect the Personal Data being transferred. For transfers between and among Allegis Group companies, we have in place a global data transfer agreement to ensure compliance with EEA data transfer rules.

b. If you need assistance with transferring Personal Data belonging to individuals based in the EEA to an external third party organization outside of the EEA, please contact your Group General Counsel.

6.9 Take special precautions with Sensitive Personal Data

6.9.1 Understanding the principle

a. "EU Sensitive Personal Data" includes information relating to an individual's racial or

ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, 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. In addition, we also treat as Sensitive Personal Data, financial Personal Data about an individual, such as their bank account or payment card details and social security numbers and national identity documentation (such as passports) (collectively this information plus the Sensitive EU Personal Data is referred to as "Sensitive Personal Data").

b. Sensitive Personal Data is subject to more stringent protection than other Personal Data, so our standards of care must be higher when dealing with this type of information.
c. When we collect and use Sensitive Personal Data, where required by law (for example for EU Sensitive Personal Data), individuals must expressly agree to the collection and use of such information. This permission to our use of Sensitive Personal Data must be freely given, specific and informed.
d. Sensitive Personal Data may be collected and used without the explicit consent of an individual where we have another lawful basis to collect and use this type of information.

6.9.2 Practical steps

a. We must always assess whether Sensitive Personal Data is essential for the proposed use.
b. We must only collect Sensitive Personal Data when it is absolutely necessary in the context of our business.
c. Where applications or other forms are used to collect Sensitive Personal Data, and where it is required by law, they must include suitable wording expressing the individual's consent, and the individual's right to withdraw consent.
d. The consent must be demonstrable. Therefore, when it is collected verbally it must be recorded in such a form as to prove that the requisite information was provided to the individual and their responses are able to be verified.
e. Where consent is not obtained, we must take steps to ensure that there is another lawful basis under applicable data protection laws for the collection and use of such information.

6.10 Comply with customer's instructions when processing Personal Data for them

6.10.1 Understanding the principle

a. In some cases, we will collect, hold and use Personal Data on behalf of our customers. Where this is the case, we must use that Personal Data only as instructed or authorized by our customers, and not for our (or anyone else's) purposes.

6.10.2 Practical steps

a. We must maintain the confidentiality and security of our customers' Personal Data at all times in accordance with our contractual obligations to them.

b. 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 to respond to that request.

6.11 Ensure service providers adopt appropriate and equivalent security measures to ours

6.11.1 Understanding the principle

a. The law requires that, where a service provider to us, including subcontractors, has access to Personal Data, we must impose strict contractual obligations dealing with the security of that information.

6.11.2 Practical steps

a. We must always enter into a written contract with any service provider, including subcontractors, that processes Personal Data on our behalf. All contracts with providers of services should include the standard contractual provisions regarding data protection made available by the Group General Counsels.

6.12 Comply with direct marketing laws and honor opt-outs

6.12.1 Understanding the principle

a. Individuals have the right to object to the use of their Personal Data for direct marketing purposes and we must honor all such opt-out requests, where any direct marketing is conducted. This applies even where individuals have previously opted-in to receiving direct marketing from us.

b. It is essential that individual's choices and preferences are accurately identified and then followed when any direct marketing campaigns are conducted.

6.12.2 Practical steps

a. We must ensure that the privacy notice made available when Personal Data is collected includes the relevant mechanisms for collecting individuals' consent to receiving marketing communications, and that it tells individuals how they may change their marketing preferences. Please contact your local Group General Counsels for further information and assistance.

b. Where we are responsible for a direct marketing campaign, we must take all necessary steps to prevent the sending of marketing materials to individuals who have opted out. In certain instances, it may also be necessary to obtain opt-in consent from individuals before sending them marketing communications – this may be the case, for example, when sending e-mail or text marketing messages. You must coordinate all direct marketing campaigns with your Marketing Department.

7 Changes to the Policy

This Policy was last updated on February 1, 2016. A notice will be posted on the Company's intranet whenever this Policy is changed in a material way.

8 Definitions

Unless otherwise defined in this Policy, all terms shall have the definition given to them under the ISO 27000 policies at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435.

9 Exception Management

If the Company determines that it has a compelling need to do so, the Company may have requirements to circumvent defined security controls set forth in this Policy.

Exceptions can be requested by contacting the Service Desk at +1-866-483-5411. Such exceptions must be escalated to and cleared by the Information Security Office in order to ensure any additional controls are put in place to mitigate risk and any residual risk is accepted by the business.

10 Comments to Policy

If you have any questions or comments about this Policy or have suggestions to improve it, please send your comments to InfoSecOffice@allegisgroup.com.

11 Revision History

Ver No.	Effective Date	Author(s) Name	Revision Description
1	November 1, 2010	Maureen Dry-Wasson and Scott Henderson	N/A
2	November 1, 2011	Maureen Dry-Wasson and Scott Henderson	Version 2
3	January 1, 2013	Maureen Dry-Wasson and Dana Pickett	Version 3
4	January 1, 2014	Maureen Dry-Wasson and Dana Pickett	Version 4
5	January 1, 2015	Maureen Dry-Wasson and Dana Pickett	Version 5
6	June 1, 2016	Maureen Dry-Wasson and Dana Pickett	Version 6 – Name of Policy changed from Privacy and Personal Data Protection Policy to Employee Privacy Policy
7	March 1, 2017	Maureen Dry-Wasson and Andrew Sheppard	Version 7 – Updated definition of Personal Data and Sensitive Data; added training and education language to enforcement section; minor typos and wording changes

12 Governance and Policy Review Management

The Information Security Office will be responsible for any changes to this Policy. The Company's Information Security Policies will be reviewed on an annual basis to ensure that it remains appropriate to the needs of our organization. In addition to the pre-defined review, the Information Security Policy will continuously evolve to meet changing internal and external requirements, which may include:

- Changes to Company's business and IT environment or tolerance to risk
- Changes to regulatory requirements
- Changes to contractual requirements, and
- Changes to adapt to emerging risks & threats

Information Security Management Framework

Records Retention Policy

Document ID - AG-ISMS-POL-07

Effective Date: 1 January 2018

Next Review Date: 1 January 2019

Table of Contents

1 Introduction

This Records Retention Policy (the "Policy") provides guidance on the retention and deletion obligations for the Company regarding Records. "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.

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 needs to 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 a number of 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 of time in order to be able to defend claims or to effectively operate our business.

Data protection and privacy law in many countries require that Personal Data, which may be a part of Records, must be kept in a form which permits the identification of individuals for no longer than is necessary for the purposes for which the information was collected or for which it is further processed. "Personal Data" means any information that relates to an identifiable individual; an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, phone numbers, email addresses, national ID (or other identification) number, job history, banking information, online identifier (like an IP address), health information, the results of background checks or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual. This may include, for example, characteristics that are unique to an individual, like a person's height, age category, regional origin or details about their profession or job function. Where the law sets specific retention periods for specific types of Records, those requirements will prevail over the deletion obligations contained in data protection law. Therefore, we will always consider whether there is an objective reason to keep Personal Data in order to justify its retention.

1.1 Document Context

This document is an integral part of the Company's Information Security Management Framework (ISMF). The ISMF provides structure to the development and maintenance of security controls in order to actively manage information security threats and risks targeting the organization's information assets.

1.2 Related Policies

The following documents are related and relevant to this document. Copies of them are available on the Company's intranet.

Ref#	Reference Document Name	Version No.	Owner/ Author
1.	Online Privacy Policy	7.0	Information Security Office
2.	Acceptable Use Policy	7.0	Information Security Office
3.	Information Security Policy	16.03.01	Information Security Office
4.	Employee Privacy Policy	7.0	Information Security Office
5.	Information Classification Policy	7.0	Information Security Office
6.	Social Media Policy	7.0	Information Security Office
7.	Bring Your Own Device Policy	1.0	Information Security Office

2 Intended Audience

The target audience of this document is Allegis Group, Inc. and its subsidiaries worldwide (referred to as the "Company"), all 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 (for example payroll providers, benefits providers, auditors, lawyers) and who have access to the Company's systems and information under contract (referred to as "Company Personnel", "You" or "you" or "Your" or "your").

3 Scope

This policy establishes a minimum level of standards, with the option for 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. This Policy applies to all Records of the Company, whether they are in electronic, hard copy or other form and regardless of their location. Records may contain Company information or third party information, such as customer, vendor or business partner information.

4 Enforcement

This Policy is important to the Company, and it intends to provide you with additional training and/or education to you to assist you in complying with it. However, where appropriate, and where additional training and/or education is not sufficient, in the event you violate this Policy, any one or all of the following further actions might be undertaken:

- 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.

5 Incident Reporting

It is important to the Company that it is aware of violations of this Policy so that it can appropriately address them, and the Company needs your help in identifying those violations. With regards to violations of this Policy:

- All violations of this Policy must be reported immediately.
- If you report violations of this Policy then you will be expected to cooperate in the investigation, however you will not be subject to reprisal or retaliation solely as a consequence of such good faith reporting or involvement.
- Retaliation is a very serious violation of this Policy and must be reported immediately.

You must report violations of this Policy as follows:

- If you are an employee, to your immediate supervisor, Records Manager or department head, and if you are a non-employee, to your Company contact person; **and**

- Online at https://infosec.allegisgroup.com/ **or**
  By telephone at +1-866-483-5411

6 Controls

6.1 Records Custodians and Records Managers

6.1.1 The person who handles and stores Records (the "Records Custodian") is responsible for the protection of those Records, including storage, retention and disposal of such records.

6.1.2 The Company has appointed and trained Records Managers, who are points of contact throughout the Company responsible for providing advice and direction regarding adherence to this Policy by the Records Custodians.

6.2 Records Retention Schedule

6.2.1 The attached Records Retention Schedule has been created and maintained by the Company in order to provide appropriate retention times for all types of Records held within the Company (see Appendix 1).

6.2.2 The retention periods set out in the Records Retention Schedule should be regarded as the default position and the maximum storage period for the listed types of Records, unless they relate to actual or threatened litigation or an investigation, in which case you should follow the process set out in section 6.3 below.

6.2.3 The retention times specified in the Records Retention Schedule have a business justification and comply with legal, regulatory or contractual requirements.

6.2.4 Allegis Group companies located in jurisdictions outside of the United States may need to create alternative Records Retention Schedules, and this is acceptable if the time periods in the Schedule are justifiable because of a genuine business need and consistent with this Policy and applicable law.

6.2.5 If a client services agreement or other contractual obligation requires that records be maintained for a period of time other than the periods of time set forth in an applicable Records Retention Schedule, the retention period in the contract will apply.

6.3 Litigation Hold Notices

6.3.1 If you receive a Litigation Hold Notice from the Company's Legal Department, 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.

6.3.2 A Litigation Hold Notice is only authorized if it is sent from the Company's Legal Department.

6.3.3 A Litigation Hold Notice will inform you that Records you may have are relevant to current or anticipated litigation, an audit, a government investigation or other similar matter.

6.3.4 If you receive a Litigation Hold Notice, you must preserve and not delete, dispose, destroy or change those Records, including e-mails, until the Legal Department tells you that the Litigation Hold Notice has been removed.

6.4 Protection of Records

6.4.1 You should maintain strict control over the storage and accessibility of Records in accordance with the Company's Information Security Policy and the Information Classification Policy, which you should consult for further information.

6.4.2 Only people who have a genuine business need to know should be able to access Records.

6.4.3 All access to stored Records must be physically and logically controlled, limited to authorized personnel only, and accessible only via proper user authentication.

6.5 Storage of Hard-Copy Records

6.5.1 Where Records are to be retained in hard-copy, in consultation with your Records Manager, you must decide whether the Records will be kept on-site or off-site.

6.5.2 Where Records are held on-site, you must ensure that the Records are properly and securely stored (for example, locked filing cabinets).

6.5.3 Where physical Records are kept off-site, the Records Manager should maintain a register of these Records and how long they should be retained.

6.6 Breach of Information from Records

6.6.1 If an information breach occurs from Records as a result of a theft, a deliberate attack on Company systems, an accidental loss or equipment failure, or some other means, it is important that the Company manages the incident appropriately.

6.6.2 In the event of an information breach, you must report it as set forth in Section 5.

6.7 Disposal of Records

6.7.1 You must dispose of Records when they reach the end of their retention period.

6.7.2 In disposing of Records, if the information is Confidential, Highly Confidential or Restricted under the Company's Information Classification Policy, you must ensure that the information is irrecoverable.

6.7.3 Hardcopy Records that include Social Security numbers or other social ID or government issued ID numbers or other Sensitive Personal Data must be cross-cut, shredded, incinerated, or pulped (for example, you can dispose of such Records in the confidential shredding bins that are provided in all Company locations).

a. "Sensitive Personal Data" includes:

i. Sensitive EU Personal Data, which is information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a national person, 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; and

ii. Personal Data the Company considers Sensitive Personal Data, which includes financial Personal Data about an individual, such as their bank account or payment card details and social security numbers/national ID numbers and national identity documentation (such as passports) (collectively this information plus the EU Sensitive Personal Data is referred to as "Sensitive Personal Data").

6.7.4 Records contained in electronic media containing Sensitive Personal Data must be securely overwritten or physically destroyed so that the Sensitive Personal Data cannot be reconstructed. In practice, some of these functions may be performed by our IS department and/or a trusted third party.

6.7.5 When Records are to be destroyed, the destruction process must cover all instances where the Records may reside, including database servers, mainframes, transfer directories, bulk data copy directories used to transfer between servers, SAN storage and paper copies.

7 Definitions

Unless otherwise defined in this Policy, all terms shall have the definition given to them under the ISO 2700 policies at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435.

8 Exception Management

If the Company determines that it has a compelling need to do so, the Company may have requirements to circumvent defined security controls set forth in this Policy. Such exceptions must be escalated to and cleared by the Information Security Office in order to ensure any additional controls are put in place to mitigate risk and any residual risk is accepted by the business.

9 Comments to Policy

If you have any questions or comments about this Policy or have suggestions to improve it, please send your comments to InfoSecOffice@allegisgroup.com.

10 Revision History

Ver No.	Effective Date	Author(s) Name	Revision Description
1	November 1, 2011	Maureen Dry-Wasson and Scott Henderson	Version 1
2	January 1, 2013	Maureen Dry-Wasson and Dana Pickett	Version 2
3	January 1, 2014	Maureen Dry-Wasson and Dana Pickett	Version 3
4	January 1, 2015	Maureen Dry-Wasson and Dana Pickett	Version 4
5	June 1, 2016	Maureen Dry-Wasson and Dana Pickett	Version 5
6	March 1, 2017	Maureen Dry-Wasson and Andrew Sheppard	Version 6 – Updated definition of Sensitive Personal Data; added training and education language to enforcement section; minor typos and wording changes

11 Governance and Policy Review Management

The Information Security Office will be responsible for any changes to this Policy. The Company's Information Security Policies will be reviewed on an annual basis to ensure that it remains appropriate to the needs of our organization. In addition to the pre-defined review, the Information Security Policy will continuously evolve to meet changing internal and external requirements, which may include:

- Changes to Company's business and IT environment or tolerance to risk
- Changes to regulatory requirements
- Changes to contractual requirements, and
- Changes to adapt to emerging risks & threats

Information Security Management Framework

Bring Your Own Device ("BYOD") Policy

Document ID - AG-ISMS-POL-08

Effective Date: 1 January 2018

Next Review Date: 1 January 2019

Table of Contents

1 Introduction

This Bring Your Own Device ("BYOD") Policy (the "Policy") explains how you are able to connect your personal devices ("Devices") to the Company's network or other resources and the remote access that the Company will have to the Devices (the "BYOD Program"). 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.

Unless otherwise stated in a separate policy that has been provided to you, the BYOD Program is entirely voluntary, and you may choose not to participate in the BYOD Program for any reason without explanation.

1.1 Document Context

This document is an integral part of Allegis Group's Information Security Management Framework (ISMF). The ISMF provides structure to the development and maintenance of security controls in order to actively manage information security threats and risks targeting the organization's information assets.

1.2 Related Policies

The following documents are related and relevant to this document. Copies of them are available on the Company's intranet.

Ref#	Reference Document Name	Version No.	Owner/ Author
1.	Online Privacy Policy	16.03.01	Information Security Office
2.	Acceptable Use Policy	7.0	Information Security Office
3.	Information Security Policy	7.0	Information Security Office
4.	Employee Privacy Policy	7.0	Information Security Office
5.	Information Classification Policy	7.0	Information Security Office
6.	Records Retention Policy	6.0	Information Security Office
7.	Social Media Policy	7.0	Information Security Office

2 Intended Audience

The target audience of this document is Allegis Group, Inc. and its subsidiaries worldwide (referred to as the "Company"), all 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 (for example payroll providers, benefits

providers, auditors, lawyers) and who have access to the Company's systems and information under contract (collectively referred to as "Company Personnel", "You" or "you" or "Your" or "your").

3 Scope

This policy establishes a minimum level of standards, with the option for 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.

This Policy applies to personal devices only. 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 or (ii) access our guest Wi-Fi network and adhere to the guest network Wi-Fi terms and conditions on a personal device without participating in the BYOD Program.

If you are using a Company issued device or a device issued to you by a client of the Company, you are subject to the Company's Acceptable Use Policy and any applicable policies issued by the Company's client for those devices.

4 Enforcement

This Policy is important to the Company, and it intends to provide you with additional training and/or education to you to assist you in complying with it. However, where appropriate, and where additional training and/or education is not sufficient, in the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Disconnecting your Device from the BYOD Program on a temporary or a permanent basis and deleting all Company data on the Device;
- 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.

5 Incident Reporting

It is important to the Company that it is aware of violations of this Policy so that it can appropriately address them, and the Company needs your help in identifying those violations. With regards to violations of this Policy:

- All violations of this Policy must be reported immediately.

- If you report violations of this Policy then you will be expected to cooperate in the investigation; however, you will not be subject to reprisal or retaliation solely as a consequence of such good faith reporting or involvement.
- Retaliation is a very serious violation of this Policy and must be reported immediately.

You must report violations of this Policy as follows:

- If you are an employee, to your immediate supervisor, or department head, and if you are a non-employee, to your Company contact person; **and**

- Online at https://infosec.allegisgroup.com/ **or**
- By telephone at +1-866-483-5411

6 Controls

6.1 Participation in and Withdrawal from the BYOD Program

6.1.1 You must consent to this Policy in order to participate in the BYOD Program, and continued participation in the BYOD Program will be considered ongoing consent to this Policy.

6.1.2 By accepting the terms and conditions of the Company during the initialization of the BYOD tools, you are agreeing to the terms and conditions of this policy.

6.1.3 If you receive a stipend for your personal device, you are expected to participate in the program and agree to the terms and conditions.

6.1.4 If you are participating, you may withdraw your consent to this Policy by deleting the BYOD Program software from the Device at any time. If you withdraw consent to this Policy, your Device will be disconnected from the BYOD Program and all Company data will be erased.

6.2 Device Security Requirements and MDM Software

6.2.1 If your Device is in the BYOD Program, it will be linked to the Company's mobile device management application (the "MDM Software"). MDM Software has the ability to identify Company data and to separate it from the personal data on your Device. Where the Company utilizes MDM Software, the MDM Software will require you to:

a. Accept the end user license terms of the MDM Software.
b. Enter a secure password and/or PIN that meets the Company's password standards prior to you accessing any Company data on your Device.
c. Change your secure password and/or PIN periodically.
d. Require your Device to automatically lock after it is idle for five (5) minutes.

6.2.2 If a Device has not been turned on for 30 days, the Company will be alerted, and the Company will disconnect your Device from the BYOD Program and erase all Company data from your Device.

6.2.3 You must keep your Device's operating system updated. The Company will support the latest two supported full versions of operating systems per device type (iOS, Android, Windows). If your Device's operating system falls below this acceptable standard, the Company will be alerted, and the Company will disconnect your Device from the BYOD Program and erase all Company data from your Device.

6.2.4 The MDM Software will inform the Company if the software on a Device has been modified to allow root access to the Device's operating system, unauthorized elevation of user privileges or circumvention of Device security measures. This is sometimes referred to as "jailbreaking" for devices running Apple iOS, and "rooting" for devices running the Android operating system. For security reasons, if the Company receives an alert of jailbreaking or rooting, the Company will automatically disconnect your Device from the BYOD Program and erase all Company data from the Device and will not allow your Device to reconnect to the BYOD Program until it is no longer in a such a state.

6.2.5 You must not attempt to modify any software installed by the Company on your Device as part of the BYOD Program. If you unenroll or remove the BYOD program software, your Device will be automatically disconnected from the BYOD Program and all Company data will be erased.

6.2.6 The Company may require you to use, apply or update anti-virus/malware protection for any Devices in the BYOD Program.

6.3 Additional BYOD Program Participation Requirements

6.3.1 Since the Device is a personal device, you are still responsible for (and the Company has no responsibility for):

a. Settling any service or billing disputes with the mobile carrier
b. Purchasing any required software not provided by the manufacturer or wireless carrier (except MDM Software as explained in this Policy)
c. Device registration with the vendor and/or service provider
d. Maintaining any necessary warranty information
e. Battery replacement due to failure or loss of ability to hold a charge
f. Backing up all personal data, settings, media and applications

6.3.2 A number of applications are recommended for use within the BYOD Program, as these applications can assist you in working remotely. Recommended applications will be sent to you by email or text. More information on these applications and an up-to-date list of all recommended applications is available on the Company's Intranet.

6.3.3 You are permitted to use your Device for work related correspondence, including email between fellow Company Personnel, clients, suppliers and other individuals or organizations. This may only be done through your Company-issued email address. You must not use personal email addresses to send or receive work related correspondence or documentation.

6.3.4 Only approved corporate applications may be used for work purposes. Any applications requiring you to create or use personal user accounts for work purposes must be approved by

the Information Security Office prior to use, be used for work purposes only and must only be linked to your Company-issued email address and not to personal email addresses or accounts.

7 Personal Data

7.1.1 At the signup stage, you will be required to provide basic personal data in order to participate in the BYOD Program. If you do not provide this information, you will not be able to participate in the BYOD Program.

7.1.2 The MDM Software will also collect and store information related to participation of the Device in the BYOD Program, including the following information:

a. Normal home country of the Device
b. Operating system and version
c. Device make and model
d. Device unique identifying number
e. Time of the last contact between the Device and the MDM Software; and
f. Time the Device was registered to the BYOD Program.

7.1.3 The Company will not use the MDM Software or sign-up 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.

7.1.4 The Company will implement appropriate technical and organizational measures with regards to the personal data collected for the purposes of the BYOD Program. Details of these measures can be found in the Company's Information Security Program policies listed in the Related Policies section.

8 Monitoring

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

8.1.2 Presently, the Company does not monitor application data on Devices. 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 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.

9 Lost/Stolen Devices and Ceasing Use of a Device

9.1.1 If a Device is lost, stolen or otherwise unaccounted for, you must inform the Company's IS Service Desk immediately by going to https://infosec.allegisgroup.com/ or by calling +1-866-483-5411. Since this is a personal device, you are advised to report the theft to the police, but whether or not to report is at your discretion. Once a report is received that a Device is lost or stolen, the Company will disconnect the Device from the BYOD Program and erase all Company data from the Device.

9.1.2 In the event that you change or stop using a Device which has MDM Software installed, you must notify the IS Service Desk, so that the Device can be disconnected from the BYOD Program and all Company data can be erased.

10 Employee Separation Management

10.1.1 On separation of employment or engagement with the Company, the Company will disconnect your Device from the BYOD Program and erase all Company data from the Device.

10.1.2 Depending on the circumstances, on commencement of a period of absence likely to last more than two weeks, the Company may elect to disconnect you from the BYOD Program and erase all Company data from the Device.

11 Definitions

Unless otherwise defined in this Policy, all terms shall have the definition given to them under the ISO 27000 policies at:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435.

12 Exception Management

If the Company determines that it has a compelling need to do so, the Company may have requirements to circumvent defined security controls set forth in this Policy.

Exceptions can be requested by contacting the Service Desk at +1-866-483-5411. Such exceptions must be escalated to and cleared by the Information Security Office in order to ensure any additional controls are put in place to mitigate risk and any residual risk is accepted by the business.

13 Comments to Policy

If you have any questions or comments about this Policy or have suggestions to improve it, please send your comments to InfoSecOffice@allegisgroup.com.

14 Revision History

Ver No.	Effective Date	Author(s) Name	Revision Description
1	March 1, 2017	Maureen Dry-Wasson and Andrew Sheppard	Version 1 – N/A

15 Governance and Policy Review Management

The Information Security Office will be responsible for any changes to this Policy. This Policy will be reviewed on an annual basis to ensure that it remains appropriate to the needs of our organization. In addition to the pre-defined review, the Policy will continuously evolve to meet changing internal and external requirements, which may include:

- Changes to Company's business and IT environment or tolerance to risk
- Changes to regulatory requirements
- Changes to contractual requirements, and
- Changes to adapt to emerging risks & threats