



CODE OF BUSINESS CONDUCT AND ETHICS

Insight Global is committed to upholding the highest standards of ethical and professional conduct. For this reason, the Company has adopted a Code of Conduct and Ethics that provides guidance to employees on upholding these standards. All employees of the Company are expected to read and uphold this Code of Conduct and Ethics.

Insight Global maintains a reporting hotline where employees or other stakeholders can submit confidential or anonymous reports of compliance concerns. Employees are encouraged to submit reports for investigation and to encourage a culture of compliance. Reports can be submitted at insightglobal.com/corporate-ethics-hotline or 1-855-260-7440.

STANDARDS OF CONDUCT

Employees of the Company are expected and required to maintain high standards of performance and conduct. While it is not possible to list all of the types of employee misconduct that can result in discipline, common sense indicates that certain types of misconduct cannot be permitted. The following list includes some (but by no means all) of the types of conduct that can result in disciplinary action, up to and including termination of employment:

- Theft or destruction of Company property or the property of other employees, managers, clients, or others doing business with the Company;
- Abusing, threatening, or intimidating other employees, managers, clients, or others doing business with the Company;
- Use of obscene, disruptive, hostile, or abusive language;
- Insubordination or refusal to perform assigned duties;
- Willful or negligent non-performance of assigned duties;
- Unauthorized use or possession of weapons, firearms, or explosives on Company or client premises;
- Excessive unexcused tardiness or absence, or failure to notify the Company of tardiness or absence in a timely manner;
- Dishonesty or falsification of Company documents or records, including (but not limited to) time records, personnel records, and employment applications;
- Reporting to work under the influence of alcohol or illegal drugs;
- Possession, distribution, sale, transfer, or use of illegal drugs on Company or client premises or while on Company business;
- Fighting or engaging in horseplay on Company or client premises;

Revised July 2022



- Accepting money, gifts, favors, loans, or other special treatment from any supplier, vendor, client, competitor, or lender of the Company, in each case in a manner that actually or would appear to impair the ability of the employee to act in the best interests of the Company, as further outlined in Section 2.06(c) of this Handbook;
- Sexual or other harassment or discrimination;
- Unauthorized disclosure of confidential business information (such as business plans or financial data) or trade secrets; and
- Violation of Company policies.

Violation of these standards of conduct or any form of disruptive or inappropriate behavior may result in appropriate disciplinary action. The nature and severity of the discipline will be determined by the Company in its sole discretion, and may reflect the severity of the violation, the employee's past record, and other individual circumstances. While the Company usually provides corrective counseling, immediate dismissal may result in situations where corrective counseling is not deemed by the Company to be appropriate to the situation.

DISCIPLINE

When an employee's performance and/or behavior do not meet the Company's standards, disciplinary action up to and including termination may result. The principal purpose of any disciplinary action is to correct the problem, prevent recurrence, and prepare the employee for satisfactory service in the future.

Depending on the severity of the disciplinary problems and completely at our discretion, the following non-exhaustive list of steps, in any combination or order, may be followed:

- Verbal Warning – A verbal warning may be given if an employee's performance or behavior fails to meet the Company's requirements.
- Written Warning – A written warning may be given if an employee fails to improve following a verbal warning or if the individual circumstances of the employee's performance or behavior warrants this level of discipline.
- Termination – An employee may be terminated if there has been no significant improvement in performance or behavior following earlier disciplinary action, or if the employee engages in serious misconduct or violations of Company policy.

The nature and severity of the discipline will be determined by the Company in its sole discretion, and may reflect the severity of the violation, the employee's past record, and other individual circumstances. Under normal circumstances, the Company will apply these levels of discipline in a progressive manner. However, any level of discipline may be applied at any time where the Company determines that it is appropriate to the situation.



ATTENDANCE AND PUNCTUALITY

The efficient operation of the Company depends upon the regular attendance and punctuality of the Company's employees. While the Company recognizes that circumstances beyond an employee's control may sometimes cause the employee to be absent from work for all or part of a day, excessive unexcused tardiness or absenteeism may result in disciplinary action up to and including termination. Excused absences are those which are taken in accordance with the Company's established PTO, sick time, or leave time policies or the law, and for which the employee gave sufficient notice to their supervisor. Unexcused absences occur when an employee fails to give the Company sufficient notice of the absence or when the employee takes time off from work in excess of that permitted under the Company's established policies or the law.

Employees are expected to be at their workstations (either in the office or when working from home) at the time they are scheduled to begin work and at the prescribed time after lunch or other breaks. An employee who will be absent from work or delayed in reporting for work by any material amount should notify their manager in advance to explain the reason for the absence or delay and the expected duration of the absence or delay. This requirement applies to each day of the absence, and habitual tardiness, even by immaterial amounts, could result in disciplinary action. Similarly, employees who need to cease work early for any reason should first obtain the permission of their manager. Failure to notify the Company of any anticipated absence or delay in reporting for work may be grounds for disciplinary action up to and including termination.

Any employee who is absent from work for three or more consecutive workdays may be considered to have resigned from their employment with the Company unless (a) the absence is excused, and (b) the employee gave the Company proper notice of the absence.

DRUGS AND ALCOHOL

The Company is committed to providing a safe, healthy, and drug-free work environment. Therefore, the Company has established the following policy:

- (1) It is a violation of Company policy for any employee to use, possess, sell, buy, transport, trade, offer for sale, or offer to buy illegal drugs or other nonprescribed intoxicants and controlled substances (or paraphernalia associated with such prohibited substances) on Company premises, during working hours, or while on the job in any capacity.
- (2) It is a violation of Company policy for any employee to report to work or work under the influence of or while impaired by illegal drugs or other nonprescribed intoxicants and controlled substances, or to report to work or work while possessing in the employee's body, blood, or urine, any detectable amount of such substances.



- (3) It is a violation of Company policy for any employee to report to work or work under the influence of or impaired by alcohol or to possess or consume alcohol on Company premises (except during Company-sponsored activities which may include the serving of alcoholic beverages), during working hours, or while on the job in any capacity, with the exception of client entertainment outings or events in which alcohol may be responsibly consumed.
- (4) It is a violation of Company policy for any employee to use prescription drugs illegally or in a manner inconsistent with the physician's prescribed dosage. It is also a violation of Company policy for an employee to be at work under the influence of prescription drugs which have the effect of impairing the employee's ability to perform their job duties in a safe and acceptable manner. (However, nothing in this policy precludes the appropriate use of legally prescribed medications that do not cause unsafe or unacceptable job performance.)

The Company reserves the right to conduct drug or alcohol tests when it believes that such tests are appropriate, including pre-employment, upon reasonable suspicion of drug or alcohol use, after an accident, after an employee returns from a substance abuse rehabilitation program, or randomly. Any testing will be conducted in accordance with applicable state law.

While the Company reserves the right to impose any disciplinary measure for a violation of this policy, an employee will ordinarily be terminated under the following circumstances:

- the employee tests positive under circumstances which would violate the above rules;
- the employee refuses to submit to testing upon request by the Company or otherwise refuses to cooperate in a Company investigation of a possible violation of the policy; or
- there is evidence which indicates, in the opinion of the Company or of the testing laboratory, that the testing sample was tampered with, substituted or altered in any way.

Additional expectations regarding the responsible use of alcohol are set forth in the Company's Policy on Alcohol Use and Related Business Activities.

CONFLICTS OF INTEREST

The Company expects and requires its employees to avoid any business, employment, or financial relationship, transaction or event which is or may be viewed (internally or externally) as a conflict of interest between an employee and an outside party. A conflict of interest exists when an employee is in a position to influence a decision that may result in a personal gain for the employee or an immediate family member (i.e. spouse or significant other, child, parent, sibling) as a result of the Company's business dealings.

An employee must promptly disclose actual or potential conflicts of interest, in writing, to their manager. Approval will not be given unless the relationship will not interfere with the employee's duties or will not

damage the Company's relationship. Similarly, employees who are unsure as to whether a certain transaction, activity or relationship constitutes a conflict of interest or who wish to seek an exception to the above rules must discuss it with the Human Resources Department, Compliance, or Legal to obtain clarification or approval.

The Company will determine, in its sole discretion, whether relationships and situations present an actual or potential conflict of interest and take steps to address the conflict of interest.

Some specific situations that can create a conflict of interest are discussed below:

A. Outside Employment

Employees are generally expected to devote their exclusive professional or business efforts and attention to the Company. Employees are required to obtain written approval from their manager before participating in any outside employment. Approval will be granted solely in the Company's discretion and only if the employment in the judgment of the Company does not conflict with the Company's interests. In general, outside employment is not allowed when it:

- prevents the employee from fully performing work for which they are employed at the Company, including overtime assignments;
- involves organizations that are doing or seek to do business with the Company's clients;
- involves job duties for another employer which would create a conflict of interest or the usurpation of opportunities related to the Company's business;
- could result in the disclosure or use of Company or client confidential information, such as client information, methods of doing business, or other material that the Company or its clients consider proprietary information or trade secrets; or
- violates provisions of law, or the Company's policies or rules.

All employees will be held to the same performance standards and will be subject to the Company's scheduling demands, regardless of any existing outside work requirements. If the Company determines that an employee's outside work interferes with the employee's work performance for the Company or the employee's ability to meet Company requirements, the employee may be asked to terminate the outside employment if they wish to remain employed with the Company.

B. Financial Interest in Other Business

An employee and their immediate family may not own or hold any interest in a supplier, client or competitor of the Company, except where such ownership or interest consists of securities in a publicly owned company and that company's securities are regularly traded on the open market, or upon the written approval of an officer of the Company following disclosure of all material facts regarding such interest by the employee.

C. Giving and Accepting Gifts

Employees are expected at all times to act in the best interests of the Company. No employee may solicit or accept gifts, entertainment or other benefits from potential or current clients, suppliers or competitors, if the item or service received would either impair the receiving employee's ability to act in the best interests of the Company or create the appearance of a conflict of interest. It is not enough that the employee avoids circumstances where there is an actual quid pro quo – each employee is expected to decline any gifts, entertainment or other services that would appear to impair their judgment or cause the employee to act other than in a fair and impartial manner, keeping the Company's best interests at heart. Under no circumstances should an employee solicit a gift from any business relationship of the Company.

Similarly, gifts and entertainment of the Company's clients should be offered in the same spirit. An employee may entertain potential or actual clients if such entertainment is consistent with accepted business practices, does not violate any law or generally accepted ethical standards, and the public disclosure of facts will not embarrass the Company. Each employee is tasked with inquiring about, and adhering to, clients' gifts and gratuities policies, if applicable. It is particularly important that employees are aware of and adhere to these limitations when doing business with state, local, or federal government representatives or with clients in specific industries, such as healthcare, where there are special rules that prohibit the gift or receipt of goods or services, even when in relatively small amounts. For example, U.S. Government employees typically may only accept gifts (including food and refreshments) valued at \$20 or less on a single occasion, and not exceeding \$50 in a calendar year. Consult the Legal Department if you are considering offering gifts or other business courtesies to Federal government employees or to government employees or any nation. Kickbacks (payments to a representative of a client in exchange for business from that client) are always prohibited.

D. Using Company Property

It is a conflict of interest for an employee to use Company facilities, supplies, property, or labor for personal gain or profit or to the Company's detriment without the express approval of the Company.

E. Diverting Corporate Opportunities

Diverting any opportunity from the Company to the employee, a relative of the employee, or any other entity constitutes a conflict of interest for that employee.

ELECTRONIC COMMUNICATIONS

The Company encourages the use of electronic communication systems because they make communication with our clients, suppliers, and each other more efficient and effective. This policy governs the use of the Company's electronic communication systems (including e-mail, voice mail, the



Internet, telephones, instant messages, and computers). Any employee who learns of misuse of the Company's e-mail, voice mail, telephone or computer systems should notify the IT Department.

A. No Expectation of Privacy

E-mail, voice mail, telephones, computers and other electronic communication systems are the property of the Company and the purpose of these systems is to facilitate the Company's business. All employees should be aware that no individual privacy or confidentiality exists in their use of the Company's electronic communication systems even when employees are issued individual passwords. Accordingly, all employees should be aware that any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring at any and all times and by any lawful means. Furthermore, the Company reserves the right to access, review, disclose or delete any user's e-mail or voice-mail communications, computer files and monitor employees' use of the Company's electronic communication systems at any time. Therefore, employees should not assume that voice mail or e-mail messages, computer files, or Internet access and usage are private or confidential.

B. Personal Use of the Company's Systems

While occasional and incidental personal use of the Company's communication systems (including voice mail and e-mail systems, Internet access, computer systems and telephones) is acceptable, excessive and/or inappropriate personal use of these systems is a violation of this Handbook.

The Company's voice mail and e-mail systems, computer systems, or Internet access should not be used to send, receive, download, or distribute communications, information or materials that are threatening, provoking, harassing, defamatory, or offensive. Examples of prohibited communications include (but are not limited to)

sexually explicit or gender-specific comments, cartoons, jokes or pictures; chain letters; unwelcome propositions of any kind; ethnic or racial comments, cartoons, jokes or slurs; or any other communication that may be reasonably construed to be harassment based upon an individual's race, color, national origin, sex, sexual orientation, gender identity, gender expression, pregnancy, religion, age, disability, service in the uniformed services, genetic information, or any other class protected by federal, state, or local law.

Employees may not use the Company's electronic communications systems: to solicit others for commercial ventures; engage in fundraising; promote religious, charitable, or political causes; or perform work for outside or personal organizations or companies, unless previously approved in writing by the employee's manager. Employees may not use the Company's electronic communications systems to





gamble. Employees also may not send chain letters or participate in any way in the creation or transmission of unsolicited commercial email ("spam"). They also may not deliberately propagate any virus, worm, Trojan horse, trap-door program code or other code or file designed to disrupt, disable, impair or otherwise harm the networks or systems of the Company or any other individual or entity.

During work time, employees may not play recreational games or maintain non-work-related blogs, Web journals or chat rooms.

Employees are not permitted to bring personal computing or data storage devices to the office or to connect them to office networks without prior approval of the Chief Information Officer. Any employee using a personal computing or data storage device on the Company's premises thereby gives permission to the Company to inspect the equipment at any time to analyze files, other data, or data storage media that may be within or connectable to the personal computing or data storage device in question. The foregoing does not apply to personal smartphones or tablets unless the employee uses the smartphone or tablet in a manner that threatens the security or confidentiality of the data resources of the Company and its clients.

C. Internet Security




Employees must comply with all Internet security rules, procedures and instructions. Bypassing of the Company's Internet firewall and other protective arrangements is strictly prohibited.

D. Data Classification

All employees are required to take appropriate measures to secure private and restricted information or trade secrets. Since no electronic communication system is completely secure, employees should use caution and good judgment when deciding whether to send or receive private or restricted business information over the Internet or using voice mail or e-mail. If there is a legitimate business need to transmit such information using an electronic communication system, such messages should only be sent to those with a legitimate business need for the information, and, if necessary, messages should be encrypted.

The Data Classification decision guide is provided below for reference:



Decision Guide	Description	Examples
Should the code, data, or document be classified as PUBLIC ?  PUBLIC	The code, data, or document has been formally approved by Legal for public use or consumption.	Public financial reporting; public website content; etc.
Should the code, data, or document be classified as RESTRICTED ?  RESTRICTED	The code, data, or document is intended only for those with a "need to know".	Code, data, or documents containing personally identifiable information (PII); payment card information (PCI); HR records; medical information; intellectual property; system designs; privacy elements restricted by law; etc.
Everything else defaults to PRIVATE even if the code, data, or document is not formally labeled		
By default, all other code, data, or documents inherit the largest classification category, PRIVATE .  PRIVATE	This is the largest bucket and by default the majority of our code, data, or documents will receive this classification, as many of them are not labeled. The code, data, or document is intended for internal use only. It is not approved for public consumption, and it is not restricted confidential.	Consider documents found on MyIG to be PRIVATE, even if they are not labeled. Do not simply download a document you find on MyIG (or cut and paste from such a document) and provide it to an external customer, or a potential customer unless you have appropriate legal protection in place. ¹
1. Please note that any document or data released or provided outside of Insight Global must be formally protected by appropriate legal protection (contract and/or NDA). If you have any questions, please contact Cyber Security & Risk.		

E. Acceptable Use Policy

Cyber Security & Risk publishes and maintains an Acceptable Use Policy ("AUP") which provides for the appropriate security of the Company (and where applicable, the Company's clients') proprietary or confidential information, intellectual property, or data that may exist in networks, systems, databases, applications, media or facilities, in either electronic or physical format.

The AUP is published and may be found by visiting MyIG, along with additional applicable IT policies.

F. Copyrighted, Trademarked and Patented Information

Employees must ensure that they respect the laws regarding copyrights, trademarks, and patents when sending information over the Internet.

G. Access to Computer, Voice Mail and E-Mail Systems

All system passwords and encryption keys must be available to the Company's management. Employees may not use passwords that are unknown to the Company or install encryption programs without turning over all encryption keys to the Company's management.



All employees (other than authorized management and supervisory personnel) are prohibited from the unauthorized access of another user's voice or e-mail messages. No employees (other than authorized management and supervisory personnel) may: (a) attempt to read or "hack" into other systems, or other user's electronic or voice mail boxes; (b) "crack" passwords or breach computer or network security measures; or (c) monitor electronic files or communications of others. Only authorized management and supervisory personnel are permitted to gain access to another user's electronic files without that user's express permission.

Employees should use strong passwords, especially when associated with accounts that provide access to restricted or private information. Employees should not share accounts or passwords, as this undermines the security of restricted and private information.

H. Use of Software

The Company purchases and licenses the use of various computer software packages for business purposes where it does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the Company does not have the right to reproduce such software for use on more than one computer. Employees may only use software on local area networks or on multiple machines according to the software license agreement. The Company prohibits the illegal duplication of software and its related documentation.

I. Working While in a Foreign Country

When employees travel and wish to work while in a foreign country, they must obtain prior authorization from their manager and Cyber Security & Risk before the date of travel. In some cases, the Company is prohibited by law from allowing the employee to work in a foreign country. For example, some contracts do not allow for the employee to continue working while in certain foreign countries. In other cases, the country may be on a government-maintained terror or watch list, which forbids certain commerce or technology. Finally, there are some countries where even having access to the Company network, or data, puts the entire Company at risk.

The IT Wireless, Mobile, & Remote Policy is published and has additional information on working remotely. The policy may be found by visiting MyIG, along with additional applicable IT policies.

REMOTE WORK POLICY

A. Purpose and Scope

The Company supports flexible work arrangements for its employees when circumstances allow and upon manager approval. As part of this flexibility, the Company may allow eligible employees to work





remotely on a regular basis, either as a fully remote employee or as part of a hybrid work arrangement where an employee splits the workweek between remote and in-person work.

The Company may also permit remote work when necessitated by a pandemic, natural disaster, or other emergency situation, sometimes on a temporary basis.

This policy applies to all internal Company employees, subject to certain limited exceptions. Permission to work a remote or hybrid schedule can be revoked or modified by the Company at any time at its sole discretion.

B. Disability Accommodation Requests

This policy does not apply to requests for reasonable accommodation for a disability under the Americans with Disabilities Act (ADA) or applicable state or local law.

Employees requesting to work remotely as a reasonable accommodation for a disability should follow the procedures outlined in the Company's Accommodations for Disabilities & Pregnancy Policy.

C. Definitions

The following definitions apply to the Remote Work Policy:

- "Hybrid working" refers to the Company's standard work arrangement where employees split their workweek between office work and remote work.
- A "hybrid employee" refers to any employee splitting their workweek between office work and remote work under the Company's standard hybrid working arrangement.
- A "fully remote employee" refers to an employee performing their entire workweek remotely with no regular workdays in the office at a Company location.
- An "office-based employee" refers to an employee performing their entire workweek in the office at a Company location with no regular workdays working remotely.

D. Eligibility

Hybrid working is the standard working arrangement for all Company employees, subject to the exceptions listed below. Unless an exception applies, employees are automatically designated as hybrid employees and do not need to make a formal request.

This hybrid work policy does not apply to:

- Fully remote employees (approved by the employee's manager).



- Office-based employees based on the employee's role or residence or other unique circumstances (designated by the employee's manager). For example, persons with responsibility to secure the company's physical office spaces generally cannot be effective when working remotely.

E. Requests to Work Fully Remote

Insight Global will consider requests to work remotely from full-time eligible employees.

A request to work remotely should be:

- In writing.
- Submitted to your direct supervisor and the Human Resources Department.
- Upon receipt of your request, the Company may contact you for additional information, including:
- An explanation as to why your job responsibilities are suitable for fully remote work.
- How you plan to stay in contact with your manager while working remotely.

Requests to work fully remote are granted at the Company's discretion, and the Company can end a fully remote work arrangement at any time.

The Company may require employees granted permission to work remotely to report to work at the Company's offices as needed.

F. Standard Hybrid Work Schedule

Hybrid employees work remotely by default but are expected to report to a Company office in-person on a regular basis as requested by the employee's manager.

The Company may require hybrid employees to report to the office on different or additional days than the standard hybrid working schedule as needed based on the Company's business or other needs, such as certain meetings, projects, deadlines, or urgent matters requiring in-person work.

Hybrid employees generally should not split a single workday between remote and office work unless special circumstances apply, which employees should discuss with their manager.

Hybrid working schedules for part-time employees depend on the part-time employee's regular hours and schedule.

Hybrid employees should consult with their manager regarding:

- Expectations about which days to report to the office and work hours.
- Work activities appropriate for office work and remote work.

- Any questions regarding an employee's particular hybrid work plan.

Hybrid employees should have open communication and transparency with their manager and team regarding schedules, locations, availability, and contact information. If an employee wishes to modify their hybrid work schedule, they should reach out to their manager.

G. Remote Work Rules

Hybrid employees must comply with all Company rules regarding remote work on the days they work remotely, as set forth below. While employees and supervisors have the freedom to develop arrangements tailored to employee and departmental needs, the following basic requirements must be met:

Schedule

The workweek for all full-time regular employees is 40 hours, divided into five days, Monday through Friday, with employees scheduled to work eight hours per day. Employees must be available to their supervisors and co-workers during core work hours, unless their supervisor has approved another arrangement in advance.

Employees must be available to attend scheduled meetings and participate in other required office activities at the Company's office as needed. Except for extraordinary circumstances, the Company normally provides at least 24 hours' notice for such events.

Duties

An employee's duties, obligations, and responsibilities remain unchanged while working remotely. Employees must be able to carry out the same duties, assignments, and other work obligations at their home office as they do when working on the Company's premises.

Working remotely is not intended to serve as a substitute for child or adult care. If children or adults in need of primary care are in the alternate work location during an employee's work hours, another person should be present to provide the care if the provision of care will unduly interfere with the ability of the employee to perform their job duties.

Compliance with Company Policies

Employees must ensure continued compliance with all Company policies while working remotely, including but not limited to the Company's policies regarding:



- Anti-Discrimination and Anti-Harassment
- Code of Business Conduct and Ethics
- Electronic Communications
- Standards of Conduct
- Time Recording
- Overtime
- Expense Reimbursement

H. Timekeeping

Non-exempt employees working remotely are required to account for all time worked in accordance with the Company's Time Recording policy. It is the remote employee's

responsibility to submit an accurate accounting of hours worked in a timely manner. Every non-exempt employee must receive advance authorization from their supervisor prior to working overtime. Non-exempt employees may not start work early, work through lunch or breaks, work late, take work home, or work overtime without the prior approval of their supervisors.

I. Payroll Taxes

It is the employee's responsibility to determine any income tax implications of maintaining a home office area. The Company will not provide tax guidance, nor will the Company assume any additional tax liabilities. Employees are encouraged to consult with a qualified tax professional to discuss income tax implications.

J. Worksite Location

If an employee plans to perform work from a location outside the state in which they currently work for an extended period of time, or if an employee plans to move from the state in which they currently work, the employee must notify their immediate manager and obtain approval prior to performing work in the other state or international location. Employees should notify their manager and request approval as soon as practicable before the employee plans to perform work in another state or international location. Employees who move must also immediately update their address in UKG. Further requirements regarding working in an international location are detailed in the Electronic Communications: "Working While in a Foreign Country" policy in this handbook.

An "extended period of time" is defined as one month or longer. A "move" is defined as a relocation of the employee's primary residence.

K. Equipment and Technology Support



The Company provides certain equipment to employees in order to perform work remotely. Any equipment supplied by the Company is to be used solely by employees for business purposes only. Employees must comply with the Company's Electronic Communications Policy and all applicable IT policies.

The Company does not provide employees with equipment or office furnishings for their home offices. Employees are responsible for equipping and maintaining their home offices so that they can accomplish their work in an efficient and expeditious manner. Employees are responsible for providing office furnishings "such as desks, chairs, and lighting" at their own expense. The Company provides common office supplies, such as paper, pens, paper clips, for employees' use for company business conducted in their home offices.

The Company will repair or replace any Company-provided equipment. However, employees are responsible for any intentional damage. The Company is not responsible for any damage to an employee's personal furniture or equipment.

Employees must return all Company-provided equipment when the remote/hybrid working arrangement ends.

The Company's technology support is available to assist employees who work remotely during normal business hours. Employees can contact the Company's technology support at servicedesk@insightglobal.com.

Employees agree that their access and connection to the Company's network(s) may be monitored to record dates, times, and duration of access.

L. Information Security

Employees must follow the Company's information security and privacy policies when working remotely, including but not limited to the Electronic Communications Policy and all applicable IT policies. This includes but is not limited to the following requirements:

- Employees must use secure remote access procedures.
- Employees must maintain confidentiality by using passwords and maintaining regular anti-virus protection and computer backup.
- Employees must not download company confidential information or trade secrets onto a non-secure device.
- Employees must not share their password with anyone outside of the Company. If any unauthorized access or disclosure occurs, you must inform the Company immediately.

Employees are responsible for securing from theft any Company property.





M. Business Expenses

The Company will reimburse employees for necessary business expenses to the extent required by applicable law. Please refer to the Expense Reimbursement policy for more information.

N. Workers' Compensation

In the event of a job-related injury, you should report the incident to your supervisor as soon as possible, following the procedures outlined in the Company's Workers' Compensation Policy. Workers' compensation does not apply to injuries to any third parties or members of the employee's family on the employee's premises.

O. Security

The employee will protect Company information from unauthorized disclosure or damage and will comply with federal, state, and Company rules, policies, and procedures regarding disclosure of public and official records. Work done at the employee's remote work site is regarded as official Company business. All records, documents, and correspondence, either in paper or electronic form must be safeguarded for return to the Company. Release or destruction of records should be done only in accordance with statute and Company policy and procedure, and with the knowledge of the employee's supervisor. Electronic/computer files are considered Company records and shall be protected as such. The employee shall surrender all Company equipment and/or data documents immediately upon request.

P. Disclaimer of Restrictions on Employees' Rights

This policy is not intended to preclude or dissuade employees from engaging in legally protected activities/activities protected by state or federal law, including the National

Labor Relations Act, such as discussing wages, benefits, or terms and conditions of employment or legally required activities.

SOCIAL MEDIA

This policy governs the use of social media (including but not limited to blogging, using Instagram, TikTok, Snapchat, Twitter, and/or Facebook, and other social media apps or forms of online commentary) by employees of the Company, whether on the Company's behalf or on the employee's behalf.

A. Compliance with the Company Policies and the Law

Before using any social media (whether on the Company's behalf or on an employee's own behalf), an employee should read and understand all of their obligations under Company policies. Among other things, certain of these policies prohibit any Company employee from disclosing any proprietary



information (such as trade secrets, information regarding the development of systems, process and products and technology) about the Company, any related entities and certain third-party entities, including our clients, vendors, and business partners. Certain of these policies also prohibit harassing or retaliating against employees, vendors, business partners, or clients of the Company. An employee must understand and obey all applicable laws relating to their use of social media, including, but not limited to, those that deal with the Company's intellectual property and financial disclosures.

B. Authorization to Use Social Media on Behalf of the Company

Only employees who have been specifically authorized to use social media on behalf of the Company as part of their jobs may hold themselves out on Social Media as representing the Company. Such employees will be given specific instructions about what may be posted on social media on behalf of the Company.

C. Using Social Media

Even if an employee has not been authorized to use social media on behalf of the Company, the employee's use of social media is still subject to this policy if the employee identifies himself or herself on that media as a Company employee and an employee discusses topics relating to the Company, its business, or its vendors, business partners, or clients. In those situations, an employee is expected to use good judgment and common sense and is required to comply with the following requirements:

- (1) **No Use of the Company's Intellectual Property:** Employees must respect all laws governing copyright, fair use of copyrighted material owned by others, trademarks and other intellectual property, including the Company's trademark, service mark or other intellectual property.
- (2) **No Disparagement:** Employees may not disparage the Company's business, vendors, business partners, or clients. This policy is not intended to preclude or dissuade employees from engaging in legally protected activities/activities protected by state or federal law, including the National Labor Relations Act
- (3) **No Harassment:** Employees may not harass, bully, intimidate, discriminate against, or retaliate against other employees, vendors, business partners, or clients of the Company.
- (4) **Tone and Topics:** Employees should not use inappropriate language (such as profanity or racial or ethnic slurs) or post offensive or pornographic pictures on social media.
- (5) **No Disclosure of Personal Information or Photographs:** Employees may not provide any personal information (such as home address or telephone number) or photographs of any Company client, employee, candidate, vendor, or business partner.

- (6) Accuracy: Employees should ensure that they are always honest and accurate when posting information or news and if they make a mistake, act quickly to correct it. Employees should also be open about any previous posts they altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. An employee should never post any information or rumors that they know to be false about the Company, its employees, candidates for employment, vendors, business partners, or competitors.
- (7) Time: An employee may not use social media for personal reasons during working hours in a manner that will unduly interfere with the performance of their work duties (although an employee may use social media for personal reasons during an employee's break time).
- (8) Press Inquiries: If an employee receives any type of inquiry from an outside source, such as a member of the press, concerning the Company's business operations (such as its products, services, business strategy, clients or vendors) in connection with an online statement that an employee has made, the person making the inquiry should be referred to Insight Global's PR and Legal Departments.
- (9) During Cyber Security Incidents: The release or disclosure of information related to a Cyber Security Incident is controlled by Legal, therefore employees should never respond to media inquiries, speculate, or comment on the matter unless specifically authorized by Insight Global's PR or Legal Departments.
 - a. Deliberate Disclosure: Deliberate disclosure of information related to a Cyber Security incident will subject the employee to discipline up to and including immediate termination of employment, subject to applicable law. In addition, conduct that is unlawful under applicable laws may subject the employee to civil, and in some cases, criminal prosecution. The Company reserves the right to refer the matter to the appropriate authorities for criminal and/or civil prosecution under applicable law.
 - b. Inadvertent Disclosure: In situations where there has been inadvertent disclosure of information related to a Cyber Security incident, employees may still be in violation of this policy and subject to discipline up to and including immediate termination of employment, subject to applicable law. Each instance will be evaluated on the facts, according to the particular situation. In addition, conduct that is unlawful under applicable laws may subject the employee to civil, and in some cases, criminal prosecution. The Company reserves the right to refer the matter to the appropriate authorities for criminal and/or civil prosecution under applicable law.



Unless an employee has been specifically authorized to speak on behalf of the Company as part of an employee's job, the employee's use of social media (including blogs and other similar forms of online communication) constitutes an employee's own, personal action and is not a Company communication. Employees will be held personally and legally responsible for their actions on social media.

INTERNAL INVESTIGATIONS AND SEARCHES

All property of the Company (including but not limited to offices, file cabinets, desks, computer files, etc.) is furnished to employees for use only as an incident of employment and solely for convenience in performing employment duties. The Company retains the right of full access to this property and may search it from time to time without further notice. The Company may also (without further notice) access Company equipment used in the course of performing job duties (e.g., computers, ipads, cell phones, or files). Furthermore, individuals may be required to display personal property (e.g. packages, purses, and vehicles parked on Company premises) for a visual inspection. Failure to permit a search can result in discipline, up to and including termination.

VIOLENCE IN THE WORKPLACE

The Company will not tolerate any workplace violence or threat of violence which occurs on Company premises or which involves or affects an employee of the Company. This policy prohibits violence or threatened violence on Company premises regardless of the relationship between the individuals involved, and off Company premises if one individual is acting as a representative of the Company or is acting within the scope of their duties, or if the prohibited behavior affects a Company interest.

Employees have a duty to immediately report any witnessed, suspected, or potential prohibited behavior to Human Resources or a manager. The Company will investigate or take other appropriate remedial action in response to any report or complaint of prohibited behavior, which may include removing or banning an individual from Company premises temporarily pending the outcome of an investigation. Reports of workplace violence will be kept confidential to the extent possible; however, certain information may be disclosed in order to conduct an appropriate investigation or to take corrective or preventative action, or to cooperate with reasonable requests of law enforcement. Employees are required to cooperate fully and honestly with investigations of possible violations of this policy.

Employees who violate this policy will be subject to discipline up to and including termination of employment. In addition, individuals who participate in a violent act or threat may be banned from Company premises and may be subject to civil liability or criminal prosecution.

Employees must provide management with a copy of any protective or restraining order that references Company premises.





If you become aware of an imminent violent act or threat of an imminent violent act, immediately contact appropriate law enforcement and then contact Insight Global's Security Department.

SOLICITATIONS

To avoid disruption of the Company's business, the following rules apply to the solicitation of funds or signatures, the conducting of membership drives, and the distribution of printed or graphic materials or literature on the Company's premises:

- (1) Non-Employees: Persons not employed by the Company may not sell or offer to sell merchandise or services or engage in any other solicitation and distribution of literature on Company premises at any time or for any purpose.
- (2) Employees: Employees of the Company may not solicit or distribute literature during working time for any purpose. The term "working time" includes both the working time of the employee making the solicitation or distribution and the working time of the targeted employee. The term "working time" does not include an employee's lunch break, authorized break times, or any other time when the employee is not required to be working. Employees may not distribute literature at any time for any purpose in working areas. "Working areas" include all areas of the Company's property where employees are performing work but do not include break areas, cafeterias, restrooms, and parking areas.

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

PROFESSIONAL APPEARANCE

As a professional services organization, our professional appearance is important to the image of the Company that we leave with clients. We expect all Company employees to use good judgment and taste in the matters of personal grooming and appearance to maintain a professional image both at the Company's offices and at the offices of our clients.

When an employee is working at a client's site, they should follow the client's dress guidelines, while at the same time maintaining a minimum standard (which in some cases surpasses that of the client). To determine what type of dress is appropriate at a client's site, the employee will need to consider the "typical" dress standard of the individuals with whom they will be interacting. For instance, if on a particular day an employee will be meeting with an officer of the company who normally wears business attire, then the employee will be expected to wear business attire.

The Human Resources Director will be the final arbiter of the suitability of an employee's attire. Employees who do not follow this policy may be required to return home to change. While employees





will be allowed a reasonable time for changing, non-exempt employees will not be compensated for this time away from work for this purpose. Nothing in this policy is intended to discriminate against natural hairstyles or textures or hairstyles associated with a sincerely held religious belief.

