LOGIC20/20
CONTRACTOR POLICIES

1. Overview

The following policies and procedures have been established to ensure that companies and individuals doing business with Logic20/20 (the "Company") and on behalf of the Company's Clients comply with the Company's policies and procedures and, when relevant, with the Company's clients' policies and procedures. Companies and Individuals doing business with the Company are defined herein as "Contractors."

2. Standards of Conduct

Logic20/20 is a professional company and involved in a highly competitive business. Clients rely on the quality and reliability of Logic20/20's services. A professional standard of conduct must be observed by all Contractors. We expect Contractors to provide excellence in their performance, meet the highest standards of integrity, exercise good judgment about their behavior, and to act in the best interests of the Company and its Clients at all times.

First and foremost, all Contractors must comply with all federal, state, and local laws and/or ordinances. Included at Exhibit A are further guidelines surrounding the Company's Standards of Conduct.

3. Information Security

The following policies and procedures have been established to protect personal and sensitive information. The Contractor shall maintain an information security management policy that is certified as compliant with all information management security system standards required by law, the Company, and/or the Company's Client. Company Client requirements will be included in any related Statement of Work. Upon a written request by the Company, the Contractor shall, at its own expense, submit to a formal audit and become certified as compliant with such standards as is required by the Company in writing. Standards of Information Security are outlined at Exhibit B. Additionally, the Contractor shall ensure that its employees are aware of and adhere to the Company's Personnel Security and Privacy Policy, as outlined at Exhibit C.

4. Social Responsibility

The Contractor shall establish and comply with a Corporate Social Responsibility policy. This policy shall include, but not be limited to statements regarding environmental, ethical, philanthropic, and economical social responsibility. Annually, the Contractor shall provide the Company with its Corporate Social Responsibility policy as well as its diversity program/policy.

EXHIBIT A
STANDARDS OF CONDUCT

Conflicts of Interest

Conflicts of Interest are an important and wide-ranging consideration. A Conflict of Interest can impact your or the Company's credibility by introducing doubt about motivations, and can lead to allegations of fraud or corruption. Therefore, you should take care to avoid Conflicts of Interest whenever possible, and to bring them to the attention of management personnel whenever you see a situation that causes concern.

A conflict of interest exists when a Contractor has an opportunity to realize personal gain from his/her/their association with Logic20/20 that otherwise wouldn't exist. It would be very difficult to define every possible example of a Conflict of Interest, but the following list includes some types of conduct that should be avoided:

- Working on behalf of Logic20/20 and/or its Clients and a competitor at the same time
- Disclosing confidential information about Logic20/20 or its clients or vendors to others and/or using confidential information about Logic20/20 or its clients for personal gain
- Borrowing money from a client
- Accepting a kickback from a client in exchange for favorable treatment
- Making a political or other donation in exchange for a promise of a favor
- Accepting substantial gifts or entertainment opportunities from clients or other outside organizations, and/or soliciting a gift in exchange for a desired business outcome
- Violating laws related to anti-trust, bribery, fraud, copyright, discrimination, etc.

Another area that can cause a perception of fraud or corruption is accepting or giving gifts. Logic20/20 believes that our clients should choose to do business with us solely based on the quality of our service, and we should choose our business relationships on the same basis. a Contractor should avoid giving or receiving any gift, gratuity, kickback, lavish meal or entertainment, etc., that could be perceived as an unfair business inducement.

In addition to the above, our Code of Conduct includes:

1 Harassment & Discrimination

1.1.1 Purpose of the Policy

Logic20/20 believes that all individuals should be treated with respect and dignity. Harassment, discrimination, and intimidation distract others from legitimate activities, harm productivity and well-being, and detract from Logic20/20's working environment and mission. Such behavior may also lead to liability under federal, state, and local laws against discrimination. It serves no useful business purpose.

Consequently, Logic20/20 expects all individuals to be treated with respect and dignity. Logic20/20 will

not tolerate any form of harassment based upon an individual's membership in any protected class (i.e., race, color, creed, religion, gender, sexual orientation or preference, national origin, age, citizenship, veteran or marital status, physical or mental disability, or any other basis protected by law). Moreover, Logic20/20 will not tolerate harassment of, or retaliation against, any individual who take actions to oppose or correct actions which violate this policy or who participate in an investigation related to potential violations.

Logic20/20 strongly encourages Contractors to report behavior which violates this policy. If a Contractor believes that he/she/they has observed or been the object of behavior which violates this policy, he/she/they should immediately report the matter to his/her/their supervisor, Human Resources, or a member of the executive leadership team (ELT). Reporting violations of this policy is a very serious matter.

Logic20/20 will investigate complaints promptly. To the extent possible, investigations will be handled confidentially. Resulting actions will depend on the nature, severity, and circumstances surrounding the incident.

This policy is only a guideline. It is intended for use by managers, employees, or contractors in preventing and correcting harassing behavior. Logic20/20 necessarily retains the sole discretion to interpret the policy as it determines is appropriate to achieve the purpose of the policy.

Because of the variability inherent in this difficult and sensitive area, nothing in this policy should be construed as a contract or a promise of specific treatment, outcome, or resolution in a specific situation.

1.1.2 Harassment Defined

Harassing conduct is prohibited whether it occurs at Logic20/20's offices, a Client's work place, Company sponsored event spaces, or at remote work locations. Moreover, it is Logic20/20's policy that all individuals are entitled to freedom from behavior in the workplace which violates this policy whether the person committing the conduct is a co-worker, supervisor, manager, or non-employee.

Sexual Harassment: Logic20/20 policy prohibits unwanted sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature. Examples of prohibited conduct include, but are not limited to: sexually oriented comments, slurs, jokes, innuendoes, cartoons, pranks, and unwelcome physical contact; unwelcome sexual advances; requests for sexual favors; use of computers for the transmission of messages or images with a sexual content; and other unwelcome verbal or physical conduct of a sexual nature.

Some additional specific examples of inappropriate behaviors include:

- Negative or offensive comments, jokes, or suggestions about another contractor or employee's gender, sexuality, or body;
- Sexual comments, jokes, suggestions, innuendoes, or gestures;
- Slang, names, or labels such as "honey", "sweetie", "boy", or "girl" that others find offensive;
- Talking about or calling attention to another contractor or employee's body or sexual characteristics;
- Displaying nude or sexually explicit or suggestive pictures, cartoons, verbiage, or calendars on any Company or organization property;

- Graphic verbal commentary about an individual's sexual prowess or deficiencies.

In addition, supervisory management, contractors, and employees are strictly prohibited from making demands for sexual favors in exchange for favorable treatment or continued work or taking any tangible work action based upon acceptance or submission to sexually oriented conduct.

Other Prohibited Harassment: Similar conduct based upon a characteristic associated with protected classes other than gender also will not be tolerated. Examples include jokes or cartoons based upon race, religion or national origin, mockery of an individual's mental or physical disability, verbal hostility towards an individual who has complained of violations of the sexual harassment policy, or racially charged pranks.

Bullying: To meet its goal of having a workplace where all individuals are treated with respect and dignity, Logic20/20 prohibits other types of unprofessional, destructive workplace behavior. For example, individuals sometimes engage in negative conduct that does not appear to have anything to do with any legally protected characteristics such as gender, race, religion, etc. One type of such abusive conduct is "bullying," and is defined as any repeated inappropriate behavior, either direct or indirect, whether verbal, physical or otherwise, conducted by one or more persons against another or others, at the place of work and/or in the course of working with Logic20/20. Logic20/20 will not tolerate bullying behavior. Logic20/20 considers the following types of behavior examples of bullying:

- Verbal Bullying: slandering, ridiculing or maligning a person or his/her/their family; persistent name-calling which is hurtful, insulting or humiliating; using a person as the butt of jokes; abusive and offensive remarks;
- Physical Bullying: pushing; shoving; kicking; poking; tripping; assault, or threat of physical assault; damage to a person's work area or property;
- Gesture Bullying: non-verbal threatening gestures, glances which can convey threatening messages;
- Exclusion: socially or physically excluding or disregarding a person in work-related activities.

1.1.3 Management & Contractor Responsibilities

All Contractors have a role in preventing and correcting behavior which violates this policy. It is the responsibility of Logic20/20 employees, contractors, and members of management to ensure a work environment exists that is neutral and free from offensive, discriminatory, and harassing behaviors. This includes off-site business meetings, engagements, and other work- related responsibilities that occur before, during, and after normal business operating hours.

All Logic20/20 employees, contractors, and members of management are required to adhere to the standards of behaviors set by this policy. All individuals are strongly encouraged to immediately report behavior that violates this policy to a supervisor, Human Resources, or a member of the Executive Leadership Team. All individuals are responsible for cooperating in investigations into violations of this policy and preserving the integrity and confidentiality of investigations into policy violations.

Supervisors and managers are responsible for monitoring the work environment and behavior of employees or contractors under their direction for compliance with the policy, including but not limited to, reporting inappropriate behavior to a supervisor, Human Resources, a member of the Executive Leadership Team, cooperating with the investigation, and participating (where appropriate) in decisions concerning the appropriate level of discipline for policy violations and taking action to prevent

recurrences of inappropriate behavior.

1.1.4 Retaliation

Logic20/20 strictly prohibits retaliation against an individual for complaining of harassment, for participating in an internal investigation, or for participating in governmental agency investigations of administrative charges of harassment.

1.1.5 Policy Violations

If Logic20/20 determines that this policy has been violated, appropriate action will be taken to ensure that the inappropriate conduct stops. Disciplinary actions and other follow up actions will depend on the circumstances surrounding the incident and the severity of the behavior, but discipline may include termination.

1.2 Anti-Corruption

Logic20/20 is committed to observing the Anti-Corruption and anti-money laundering laws, including the Foreign Corruption Practices Act (FCPA), of the states and country in which it conducts its business. Logic20/20 prohibits payments of bribes or kickbacks, in any form, whether in dealings with individuals and clients in the private sector or public officials and their representatives.

1.2.1 Money Laundering

Money Laundering is strictly prohibited by all Logic20/20 Contractors. No Contractor shall use their relationship with Logic20/20 to manipulate, hide, disguise, or purposefully misclassify any sources of income or expenses.

1.2.2 Client Relationships

Logic20/20 Contractors are prohibited from engaging in corrupt practices with client representatives, including bribery and kickbacks, before, during, and after client engagements, for both private and public sectors. No Contractor may authorize, assist, or conspire with another individual to violate anti-corruption laws or this policy.

1.2.3 Compliance

All Logic20/20 Contractors are to adhere to and observe all applicable Anti-Corruption laws including the Foreign Corruption Practices Act (FCPA). No Contractor is authorized to promise, authorize, offer or pay anything of value (including but not limited to gifts, travel, hospitality, entertainment, charitable donations, privileges, or employment) to any individual in the private or public sector, whether directly or indirectly.

1.3 Safety

It is our goal to provide and maintain safe working conditions for all individuals, to follow safe operating procedures, and to comply with all safety laws and ordinances. Please be on guard for any unsafe conditions and report any problems immediately to your supervisor and Human Resources. Prevention is the key, and ordinary common sense is the best approach.

1.3.1 Workplace Violence

Logic20/20 does not tolerate any type of workplace violence committed by or against any individual. Contractors are prohibited from making threats or engaging in violent activities. This includes making jokes about committing any sort of violent act, as well as bringing in material that, even if it is meant to be comic in nature, could be construed as a physical threat to coworkers. The following list of behaviors, while not exhaustive, contains examples of conduct that is prohibited:

- Causing physical injury to another person
- Making threatening remarks
- Engaging in aggressive or hostile behavior that creates a reasonable fear of injury to another person
- Intentionally damaging employer property or the property of another employee
- Possessing a weapon while on company property or while on company business
- Committing acts motivated by, or related to, sexual harassment or domestic violence

Any potentially dangerous situations must be reported immediately to a supervisor and to Human Resources. Reports can be made anonymously and all reported incidents will be investigated.

Reports or incidents warranting confidentiality will be handled appropriately and information will be disclosed to others only on a need-to-know basis. Logic20/20 will intervene as appropriate to a possibly hostile or violent situation. **In any case of imminent or actual physical threat, employees should call 911.**

1.3.2 Drug & Alcohol Policy

The company recognizes that substance abuse is one of the major health problems in our nation today. Drug and alcohol use on the job leads to impaired judgment, poor performance, higher accident rates, sickness, absenteeism, and poor morale.

Logic20/20 prohibits coming to work, performing work-related responsibilities and duties, or operating company equipment under the influence of illegal drugs, marijuana, alcohol, or other intoxicants. It is our policy to maintain a drug-free workplace. Contractors' compliance with this policy is important for their own benefit and for the benefit of their co-workers. This policy does not prohibit the lawful and responsible consumption of alcoholic beverages served at a Logic20/20 social function or during appropriate business entertainment.

If a Contractor is suspected of reporting to work under the influence of alcohol, marijuana, illegal drugs, or other intoxicants, the Company will discuss the suspicion with the Contractor and retains the right to request immediate drug testing.

If there is reason to believe at any time that an Contractor is violating any aspect of this policy, then they may be asked by the Company to submit immediately to a search of his/her/their person, work area, vehicle and/or other personal belongings. Entry into the Logic20/20's premises constitutes consent at Logic20/20's discretion to conduct searches and inspections. Refusal to consent to a search or inspection constitutes insubordination and violation of company policy.

1.3.3 Drug Testing

A Contractor may be asked to complete a drug test if a client requires its completion for purposes of performing services for them. A Contractor may be required to undergo substance testing by the company under either of the following three conditions: (1) there is reasonable cause to suspect that the Contractor has reported to work or is working under an impaired condition as a result of drug, intoxicant or alcohol use; (2) the Contractor has been involved in a job-related accident or an apparent violation of a safety rule or standard has occurred, or (3) the client's policies (on a project where the Contractor will be engaged) requires that such testing occurs.

The testing of A Contractor requires approval of Human Resources or a member of the Executive Leadership Team[2]. If the employee tests positive, then confirmation analysis shall be sought through an outside laboratory designated by the company and meeting federal requirements.

1.4 Mandatory Training

Logic20/20 Contractors must complete training modules deemed to be mandatory by Logic20/20 or their clients within the stated timeline. Logic20/20 reserves the right to select other required trainings for employees at any time.

EXHIBIT B
STANDARDS OF INFORMATION SECURITY

a) Annual Risk Assessments

The Contractor shall conduct an annual security risk assessment and provide the results of that assessment to the Company within 30 days of completion.

b) Network Vulnerability Scans

It is expected that all support of applications containing sensitive information will occur on the Company's client's infrastructure and will therefore be subject to client standard scanning policies and associated schedules. Should the Contractor become aware of sensitive information not being maintained solely on the Company's Client's infrastructure, it shall notify the Company immediately.

c) Prevention of Unauthorized Access

The Contractor shall establish industry-standard processes and policies to prevent unauthorized access to its facilities and/or information systems.

d) User Permissions Access

The Contractor shall enforce a policy of 'least privilege'. Permissions exceptions must be approved by designated personnel. Written record of these approvals shall be appropriately maintained.

e) Anti-virus and anti-malware protection software Policy

All equipment connected to Logic20/20 or Client networks must have antivirus and antimalware software installed. Such software shall be updated and maintained in a timely matter.

f) Resolution of complaints and requests relating to security issues

The Contractor shall maintain a defined complaint process which is used for reporting both security and other complaints.

g) Errors and omissions, security breaches, and other incidents

The Contractor shall establish a security breach policy and comply therewith and make this available to the Company upon its request.

h) Intrusion Detection

Applications containing Personal or Sensitive Information are hosted on client infrastructure and are subject to all client intrusion detection policies and processes.

i) Exception Handling

The Contractor shall have processes and procedures to handle Security exceptions. Exceptions to policies and procedures shall be appropriately documented, reviewed and approved.

j) Processing integrity and related system security policies.

The Contractor shall maintain a defined Processing Integrity Policy and associated checklist and make this available to the Company upon its request.

k) Disaster Recovery

The Contractor shall maintain a business continuity and disaster recovery plans and make this available to the Company upon its request.

l) Authentication

All end users shall be allocated unique user ID's and passwords for on-line access to information.

For online authentication, Contractor employees must:

1. Use a client-provisioned account
2. Require that an individual use a unique ID and password (or equivalent)

If a Contractor employee is terminated, the Contractor shall deactivate network and all other support accounts for anyone no longer working on programs within 24 hours of users leaving the program and within 2 hours for non-voluntary dismissal. In those instances, where clients must remove access, affected clients are notified within these same timeframes. Removal of access includes internal/external access, media, paper, technology platforms, and backup media.

m) Destruction of Personal Information

When the destruction of client Personal Information is necessary, Contractor must:

1. Burn, pulverize, or shred physical assets containing Personal Information so that the information cannot be read or reconstructed. Shredding bins are available on-premise for these purposes.
2. Destroy or erase digital assets containing ClientPersonal Information so that the information cannot be read or reconstructed.

n) Protection of Digital Assets

The following steps are outlined to protect personal information transmitted over the Internet or other public networks. Contractor must:

1. Employ industry standard encryption implementations of SSL, TLS, or IPsec for Client Information in transit and for sender/receiver authentication.
2. Employ BitlLocker drive encryption (or an equivalent industry recognized alternative) on any laptop on which information is stored or accessed.
3. Promptly investigate breaches and attempts to gain unauthorized access to systems containing Client Personal Information.
4. Promptly communicate investigation results to management and IT personnel and notify Logic20/20 of these investigations.

o) Testing and Audits

Regarding testing and audits, the Contractor shall:

1. Regularly test the effectiveness of the key safeguards protecting Personal Information. Documentation of testing and test results is required as are modifications to systems, policies and procedures when test results identify shortcomings.
2. Periodically undertake independent audits of security controls. When required per Client contractual terms, security audits must be conducted in accordance with contract terms.
3. Make the results of these audits available to the Company on request.
4. Periodically undertake threat and vulnerability testing, including security penetration reviews.
5. Anonymize all Client Personal Information used in a development or test environment.

EXHIBIT C
PERSONNEL SECURITY AND PRIVACY POLICY

1 Use of Equipment & Supplies

Logic20/20 provides Contractors with supplies and equipment to perform their tasks. These are to be used for Logic20/20's business only. Contractors are not permitted to use Logic20/20 supplies or equipment for their personal use.

Contractors are expected to know how to use equipment supplied by Logic20/20 to perform their duties. For security reasons, Contractors must use the company-provided laptop for all work performed for Logic20/20 unless otherwise specified in a Statement of Work (SOW), or explicitly approved by the Company's IT Director.

Contractors are to use Logic20/20 equipment properly and for its intended purpose and are expected to return all equipment to Logic20/20 in good working condition. Contractors must notify their supervisor if they find that any equipment is not working properly or in any way appears unsafe.

1.1 Document Creation & Storage

Artifacts created while employed by Logic20/20, including but not limited to documentation and code, are the intellectual property (IP) of Logic20/20. All documents should be stored on approved cloud-based storage media (typically OneDrive or SharePoint for internal Logic20/20 documents). Contractors should seek guidance from their Project Manager, Engagement Manager, or Executive In Charge (EIC) for project-specific storage and collaboration guidelines.

1.2 Software Licensing & Copyrights

Logic20/20 prohibits the use of any unlicensed software. All software must be approved and procured by a member of the IT Team before being installed.

1.3 Proprietary Property/Non-Disclosure

Contractors may have access to information which is considered confidential and propriety to Logic20/20.

Such information consists of, but is not limited to:

- The names of Logic20/20's customers, Logic20/20's financial information, rates, services, contract terms, and marketing plans
- Logic20/20's computer systems, including computer hardware, computer software, and the unique methods and techniques used by Logic20/20 in applying the same
- Developments, improvements, and inventions that are produced by Logic20/20 in the course of its business

Contractors shall not disclose to any person any portion of Logic20/20's confidential information except as specifically authorized by a supervisor. In addition, Contractors shall not (a) make any use of the Logic20/20's confidential information except for uses necessary to his/her/their work for Logic20/20; or (b) use Logic20/20's confidential information for his/her/their own personal benefit.

Contractors will take every commercially reasonable measure to protect the privacy, security and integrity of all client data. Contractors will not make unnecessary copies of data and will ensure data is stored only on company-approved devices and network shares/sites. Under no circumstances can Contractors make data available on a website, ftp site, email, or any other method without ensuring it is encrypted, and that access to that device or location can only be accessed using a secure authentication token. Non-secure information, such as product builds, can be published without encryption, but should still be made available only to appropriate parties, and via a method that requires them to authenticate.

1.4Use of Company Internet, Email, & Phone

1.4.1 General

The following policies apply to all electronic communication used by the Contractors of Logic20/20. Misuse of email, the Internet, and other electronic data can have serious legal ramifications.

- *Computer Data Is Not Private:* All electronic data stored on computers at Logic20/20's offices, electronic data stored in the One-Drive and other Logic20/20 cloud sites, and all electronic data stored on laptops provided by Logic20/20, is the property of Logic20/20. As such, Logic20/20 retains the right, but not the duty, to monitor, read, and review any electronic data stored or created on any user's computer or laptop, including but not limited to word processing documents, graphic files, email sent or received by Contractors, Internet links and Internet (HTML) files. Computer users waive any right to, or expectation of, privacy with respect to any such files created, stored, sent or received.

- *Obscene, Harassing, and Offensive Materials:* Contractors shall not create, store or knowingly access computer files or other electronic information containing obscene, harassing or otherwise offensive content. This includes files on computers at Logic20/20 as well as those accessed through the Internet.

- *Financial Gain and Illegal Activities:* Contractors shall not use Logic20/20 computers for personal financial gain, or in connection with illegal activities. Such prohibited use includes but is not limited to email communications and Internet use.
- *Personal Use:* Personal use of a Logic20/20 computer, Internet address, or Logic20/20 online access account is to be kept to a minimum and shall not interfere with Logic20/20 business needs. It is expected that Logic20/20 Contractors will limit their use of internet access to business issues only during working hours. Logic20/20 reserves the right to monitor all use of Logic20/20 computer resources.

1.4.2 Specific Email & Instant Messaging Policies

Although email and instant messaging are fast and efficient ways to communicate, they must be used with care, common sense, and good judgment. Since Logic20/20's name is part of the Contractor's email address, email can make every user appear to be a spokesperson for Logic20/20. Because both Logic20/20 and its Contractors can be held liable for the content of their email, the following are Logic20/20 policies which have been adopted to enable us to enjoy the efficiencies of email without putting Logic20/20 or its employees at risk.

- *Retrieval and Response*: Failure to respond promptly to email or instant messages carries the same implications as failure to respond promptly to a phone call. It is the responsibility of every Contractors to check their Logic20/20 and client emails regularly during the workday. If a Contractor is out of the office, the out-of-office message assistant must be turned on and contain alternative contact information.
- *Harassment and Discrimination*: Email and instant messages are subject to the same laws as face-to-face and other communications. Contractors are strictly prohibited from sending email messages of a discriminatory, harassing, intimidating, offensive or rude nature. Email should never contain language which would be considered unacceptable if spoken in a normal business setting, and should convey the same respect, restraint, and professional decorum as displayed in face-to-face communications.
- *Receipt of Improper Email*: If Contractor receives material via email or instant message whose content is in violation of this policy, it is the Contractor's responsibility to delete the material from their computer, ask the sender to desist from sending such material, and report the incident to a supervisor.
- *Email Security*: Email by default, should not be considered a secure medium for communication of confidential or PII information. Confidential communication should not be sent via unencrypted email. Passwords associated with email access must be kept private to prevent unauthorized communication.
- *Mobile Devices*: Access to company email on personal mobile devices must be done in compliance with Logic20/20's Mobile Device Use Policy (included in item 1.4.4 below).

1.4.3 Internet Use Policies on Logic20/20 Devices

Permitted Purposes: The sole purpose for which Contractors may access the Internet is to carry out Logic20/20's legitimate business purposes. Every connection made on the Internet can be traced back to

the originator, leaving a trail of “business cards” easily tracked by others back to Logic20/20. Therefore, do not visit any sites where you or Logic20/20 would be reluctant to
leave your “business card.”

Permitted Use; No Privacy Expectations: The only persons who may access the Internet are Logic20/20 Contractors and such other persons as Logic20/20 may specifically authorize. Logic20/20 reserves the right to access and disclose, for any lawful purpose, the contents of any Internet messages sent to and from Logic20/20’s computer equipment including email. All users, including Logic20/20 employees, using the Internet waive any right to privacy in such messages, and consent to their being accessed and disclosed by Logic20/20 personnel.

1.4.4 Mobile Device Policy

When connecting via a mobile device to Logic20/20’s email system, the policies below must be followed:

- A 4-character (or longer) numeric password will be required
- Sign-in will be required after 10 minutes of inactivity
- In the event that a device is lost or stolen, a member of the ELT should be notified immediately. All contents of your device will be wiped (deleted).

Accessing Logic20/20 email from your mobile device is voluntary. Access will be denied for any Contractor attempting to connect to work email via a device that will not or cannot support the above policies. All current and recent iPhone, Windows and Android devices are capable of supporting these policies.

1.5 Information Security Policy

Logic20/20 needs to maintain the confidentiality of Personal Identity Information (PII) and understands that such information is unique to each individual. The PII covered by this policy may come from various types of individuals performing tasks on behalf of the Company and includes employees, applicants, clients, and independent contractors. The data covered by this policy includes, but is not limited to, all electronic information found in e-mail, databases, applications, and other media as well as paper information, such as hard copies of electronic data and employee files. The scope of this policy includes company requirements for the security and protection of such information throughout the Company and its clients and applies to all employees , Contractors, and vendors who may have access to the Company’s or Client’s data.

1.5.1 PII Definition

PII is any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. It also refers to any information from which identification or contact information of an individual person can be derived. Forms of PII can include but are not limited to:

- Address, both physical and email
- Social Security Numbers (or their equivalent issued by governmental entities outside the United States).
- Taxpayer Identification Numbers (or their equivalent).
- Employer Identification Numbers (or their equivalent).
- State or foreign driver's license numbers.
- Date(s) of birth.
- Corporate or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records.

1.5.2 Data Types

Logic20/20 interacts with two main kinds of data:

- Company-owned data that relates to such areas as corporate financials, employment records, etc.
- Private data that is the property of our clients and employees, such as credit card information, social security numbers, contact information, etc.

1.5.3 Data Access

Logic20/20 maintains multiple IT systems where PII data may reside; thus, user access to such IT systems is the responsibility of the IT department. The IT department has created internal controls for such systems to establish legitimate access for users of data, and access shall be limited to those approved by IT based on a documented security plan. The IT department has created physical and logical access controls to prevent unauthorized access, but will on occasion conduct tests to detect unauthorized access, attempted attacks, or system intrusions as well as proactively test security procedures. Any change in vendor status or the termination of an employee or Contractor with access will immediately result in the termination of the user's access to all systems where the PII may reside.

1.5.4 Data Transmission & Transportation

Company Premises Access to PII: IT has oversight responsibility for all electronic records and data access capabilities. Human Resources has the operational responsibility for designating initial access and termination of access for individual users within the company and providing timely notice to IT.

Local Access to (PII): In the course of doing business, it may be necessary to download PII data to laptops or other computing storage devices to facilitate company business. To protect such data, any such devices are required to use IT department-approved encryption and security protection software (typically BitLocker) while such devices are in use on- or off- company premises.
The IT department has responsibility for maintaining data encryption and data protection standards to safeguard PII data that resides on these portable storage devices. It is a violation of Company policy to tamper with or disable encryption on any Company-provided device.

1.5.5 Client Security Policy Compliance

At the start of every client project, each team member is responsible for reviewing the client's data protection policy and requirements to ensure that they are familiar with and can comply with the client's data security expectations and processes in totality. There may be additional

policies to which project teams need to adhere in order to fully comply with the client's policy. All Logic20/20 team members are required to fully comply with all client policies, including those concerning the protection of client-owned PII.

Contractors are prohibited from working with client PII unless it is absolutely necessary for the successful completion of the project. All effort should be made to fulfill project objectives without the use or storage of PII by the Logic20/20 project team.

If a Contractor is given access to data containing client PII, then they need to notify his/her/their engagement manager immediately. The engagement manager should then notify the client project sponsor that the team is in possession of PII, and explain the steps the team will take to ensure its privacy and its destruction upon the conclusion of the project. All PII must be used for its intended purpose in the project only.

Unless absolutely necessary, client PII should never be emailed to and from project team members or stored on Logic20/20 laptops or other Logic20/20 sites. Instead, it should be stored on client internal servers or SharePoint sites that have been approved by the client's IT department as having the appropriate level of security and encryption in place to keep the data protected. Use of sensitive or confidential information across projects is strictly prohibited.

Regardless of where the PII data is stored, the Executive in Charge of the engagement is ultimately responsible for its safe storage and its return or destruction immediately after the project concludes. Any PII data must be secured in a safe location at all times, and all copies of the data must be permanently deleted or otherwise destroyed immediately upon the conclusion of the client project. Engagement managers should be prepared to provide a sworn attestation that the data has been irrevocably destroyed if asked by the client or Logic20/20 Human Resources.

1.5.6 Data Breaches & Notification

Documents, databases, or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, the company will notify all affected parties whose data may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible. The Legal department will handle breach notifications(s) to all governmental agencies to whom such notice must be provided in accordance with time frames specified under these laws. Notices to affected individuals and clients will be communicated by Human Resources after consultation with the Legal department and within the time frame specified under the appropriate law(s) and service agreements. Refer to the Breach of Privacy Report Process for more information. Contractors are required to fully cooperate with any investigation stemming from a notification of a potential breach.

1.5.7 Audits

Periodically Logic20/20 will undertake independent audits of security controls, including network penetration testing, patch scanning, and safe word testing, to ensure that encryption and security controls are working properly. Logic20/20 will also conduct regular audits of PII maintained by the Company to ensure that this policy remains enforced. Where the need no longer exists, PII information will be destroyed in accordance with records retention policies and applicable protocols for destruction of such records. Logs are maintained with the dates of destruction.

1.5.8 Complaint Process

If any client, employee, vendor, or contractor has any concerns that company representative(s) are not adhering to the provisions of this policy, they should contact the Human Resources. All concerns will be investigated and resolved within thirty days, and the complaint and resolution process will be documented and shared with the Logic20/20 Executive Leadership Team and appropriate client resources. Refer to the Breach of Privacy Policy for more information.

1.5.9 Required Measures for Keeping Data Private & Safe On Your Device

- Never leave your laptop in your car
- Immediately report any lost or stolen items to Logic20/20 Human Resources or the IT Manager
- Install all computer software updates required by Windows Update
- Lock your notebook every time you leave it (WIN+L), and ask the IT department for a laptop lock if you regularly work in public areas
- Use complex passwords, and never share them or write them down
- Never leave your laptop or accessories unattended, including conference rooms, kitchen/lunch rooms, or any other public space.

<u>On Logic20/20 projects</u>

- Respect building access policies: do not “tailgate” into office buildings, and do not let others tailgate into buildings behind you
- Only collect the client information you need to fulfill project requirements
- Dispose or return sensitive information immediately upon conclusion of the project
- Escalate any problems or security-related issues to the project’s engagement manager or to Logic20/20 Human Resources
- Do not share sensitive or confidential information across client projects
- Encrypt all data before transferring it to another team member

<u>At Logic20/20 office locations:</u>

- Remember that while Logic20/20’s offices have access controls in place 24x7, all employees should take the necessary precautions to protect their and Logic20/20’s

property
- Do not discuss confidential information in open areas
- Lock your computer's screen when you step away from it
- Tuck purses and other personal possessions out of sight

1.6 Social Media

In the rapidly expanding world of electronic communication, social media can mean many things.

Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with Logic20/20, as well as any other form of electronic communication.

Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Ensure that all of your postings are consistent with Logic20/20's policies.

1.6.1 Be respectful, honest, & accurate

Always be fair and courteous to fellow employees, customers, vendors or other people who work on behalf of Logic20/20. Use of statements, photographs, video, or audio that could reasonably be viewed as malicious, obscene, threatening, or intimidating, or that might constitute harassment or bullying are prohibited. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination. Examples of such conduct might include posts that could contribute to a hostile work environment.

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered.

Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about Logic20/20, its employees, Contractors, clients, vendors or other people working on behalf of Logic20/20 or its competitors.

1.6.2 Post only appropriate & respectful content

Maintain the confidentiality of Logic20/20's and its customers' trade secrets and proprietary information. Trade secrets may include information regarding the development of systems, processes, products, know-how, and technology. Do not create a link from your

blog, website or other social networking site to the Logic20/20 website without identifying yourself as an employee of Logic20/20.

Express only your personal opinions. Never represent yourself as a spokesperson for Logic20/20. If Logic20/20 is a subject of the content you are creating, be clear and open about the fact that you are a Contractor and make it clear that your views do not represent those of Logic20/20, fellow employees, Contractors, clients, vendors or other people working on behalf of the Company.

If you do publish a blog or post online related to the work you do, or to subjects associated with Logic20/20, make it clear that you are not speaking on behalf of the Company. It is best to include a disclaimer such as: “The postings on this site are my own and do not necessarily reflect the views of Logic20/20.”

1.6.3 Use of social media at work

Refrain from using social media while on work time or on equipment the Company provides, unless it is work-related as authorized by your manager and otherwise consistent with the Company equipment policy. Do not use Logic20/20 email addresses to register on social networks, blogs or other online tools for personal use.