IASIS HEALTHCARE	**POLICY TITLE**: **Confidentiality & Security Agreement**
MANUAL NAME: Information Security Manual	**POLICY NUMBER**: SEC.008.1 ☐ Addendum to Corporate Policy ☐ Form Available In I-REPP System
SECTION (as applicable):	**POLICY OWNER**: Chief Privacy/Information Security Officer
ORIGINATION DATE: April 13, 2003	**FINAL APPROVAL DATE**: September 12, 2016

POLICY:

IASIS and its affiliates, hereinafter referred to as the Company, stores, processes, and disseminates large amounts of critical/sensitive information. The Company has a legal and ethical responsibility to safeguard the privacy and confidentiality of Protected Health Information and confidential information. The loss, damage, or disclosure of such information or any Information Resources (as defined below) could result in a significant harm to the Company. It is imperative to ensure the integrity, accuracy, availability, and confidentiality of these Information Resources through the use of effective security controls. It is every user's responsibility to guard against unauthorized use, destruction or disclosure of the Information Resources and to protect the Company's information and Information Resources.

SCOPE:

All Company-affiliated facilities' workforce members, providers, providers' staff including but not limited to, hospitals, ambulatory surgery centers, home health agencies, physician practices, vendors granted access to IASIS confidential information and all Corporate Departments, Divisions and personnel.

DEFINITIONS:

"Confidential Information" includes, but not limited to, Protected Health Information, human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers.

FISO – Facility Information Security Officer

"Information Resources" include, without limitation, all IASIS owned or provided:

- electronic and printed data and documentation;
- online screen transactions;
- software applications;

- data set files and databases residing in any media, such as tape, all storage disk (i.e., external / internal hard drive, USB Flash / Thumb Drive, Pen Drive), CD's, microfilm, and microfiche;
- smartphones, iPads and PDA's;
- processing systems to include servers, PCs, workstations, and printers; and
- network resources.

PHI – The HIPAA Privacy Rule protects most "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral. The Privacy Rule calls this information *protected health information* (PHI). Protected health information is information, including demographic information, which relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

"Workforce Member" includes employees, contractors, volunteers, independent contractors, trainees and other individuals (e.g., vendors) who in the performance of work for the Company , are under the Company's direct control and who have access to Confidential Information.

PROCEDURE:

All Company workforce members, providers, providers' staff and vendors, hereinafter referred to as "users", who are granted access to any of the Company's Information Resources are responsible for safeguarding the confidentiality and integrity of the Information Resources to which (s)he has access. By signing the IASIS Confidentiality and Security Agreement (CSA) (Attachment A, B or C) the user acknowledges this responsibility.

A. Information Confidentiality and Security Agreements with Individuals.
   1. Users who are granted access to Company information, or granted access to Company provided systems must sign and abide by the CSA. All Company affiliated physicians granted access to Company information, or granted access to the Internet through Company provided systems, must sign and abide by the Provider Confidentiality and Security Agreement (Provider CSA). All Company vendors and their staff granted access to Company information, or granted access to the Internet through Company provided systems, must sign and abide by the Provider Confidentiality and Security Agreement (Vendor CSA). The CSAs acknowledge specific responsibilities the individual has in relation to information security and the protection of confidential information, including confidential patient information, from unauthorized disclosure. These individual obligations support federal regulations for confidentiality and security, including the HIPAA Privacy and Security Rules.
   2. A non-Company owned physician practice, vendor, or other external entity may make and shall enforce such CSAs on behalf of employees working off-site (e.g., contracted transcription service, electronic claims submissions support contractor, physician office practice), if stipulated in the Company's contract with the external entity (see B. below). Each individual working on Company premises accessing Company and/or patient information must sign a CSA.

3. The CSAs are official corporate documents and must not be altered in any manner without prior approval from the CIO and CCO.

B. Business Associate Agreement (BAA) with Business Partners/Associates:
Relationships with an external entity involving access to Company information and Company information systems or the exchange, transmission, or use of sensitive Company information that meet the HIPAA definition of a business associate require a formal contract and BAA including provisions to protect the confidentiality and security of the information and/or systems.

1. A Company representative authorized to approve access to the Company information system and/or the disclosure of the sensitive Company information must sign the BAA.
2. The BAA must include provisions governing the entity's information security policies and practices, as well as requirements to support Company compliance with regulatory requirements.
3. Current required Contract provisions are provided by the Legal Department.

C. External Entity or Vendor:
Relationships with an external entity involving access to Company information and Company information systems or the exchange, transmission, or use of sensitive Company information that do not meet the HIPAA definition of a business associate require a formal contract including provisions to protect the confidentiality and security of the information and/or systems.

1. A Company representative authorized to approve access to the Company information system and/or the disclosure of the sensitive Company information must sign the Contract.
2. The Contract must include provisions governing the entity's information security policies and practices, as well as requirements to support Company compliance with regulatory requirements.
3. Current required Contract provisions are provided by the Legal Department.

C. Sanctions:

Violations of this policy could lead to disciplinary measures up to and including termination of employment or business relationship. Suspected violations of this policy are to be handled in accordance with the Discipline section of the IASIS Code of Conduct. The Company encourages resolution at the local level and each Customer (an organization, business entity or organizational unit that has an established business relationship with IASIS as described in this policy's scope) will designate a process for reporting violations. In addition, violations may be reported to the IASIS Alert Line at **1-877-898-6080**.

D. Policy Exceptions.
Exceptions to Security Policy are to be submitted to IASIS CIO for review and approval.

E. Each Company workforce member must sign the CSA at the time of employment or engagement, before access to Company information or Company systems is granted. The completed CSA is maintained in by the appropriate department based on the facility's process.

F. Each physician and allied health professional must sign the Provider CSA (Attachment B) at the time (s)he is initially appointed to a facility's medical staff. Completed Provider CSAs will be maintained in the individual's credentials file.
Completed Provider CSAs for members of the Provider's staff must be maintained in a central location designated at the local level.

1. Providers must assign each member of their office staff a unique user ID to access Company systems, which is generated in accordance with Company procedures.
2. Providers must notify the FISO or designee within 24 hours or by the next business day about terminated office staff to ensure that their staff's user accounts to Company systems are appropriately disabled in accordance with Company standards and procedures for account termination.

G. Representatives of vendors and other external entities must sign the CSA (Attachment C) at the time information access or system access is granted. Completed CSAs must be maintained in the individual contract folder by the Facility CFO or designee.

H. All individuals listed in items A-G above are required to re-sign the CSA when Corporate Information Security makes significant revisions to the CSA and those revisions are approved by the CIO and CCO.

FORM REFERENCES:

SEC.008.A – Confidentiality and Security Agreement
SEC.008.B – Provider Confidentiality and Security Agreement

REFERENCES:

CFR 45 §164.310(a)(2)(iii)

Review/Revised Date:	Title:	Description of Change or Location of Change in Document:
September 7, 2016	CP/ISO	Changes to address external entities and vendors. Addition of Attachment C
June 22, 2016	CP/ISO	Template/reformatting. Biennial review, add definitions, add attachments

ATTACHMENT A

IASIS Confidentiality and Security Agreement

Note: this form is for IASIS workforce members

I understand that the IASIS affiliated facility or business entity (the "Company") for which I work, volunteer or provide services, manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their protected health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment/assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the IASIS website (under Employees / IREPP). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company systems.

General Rules

1. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
2. I will immediately report to the Company any suspected unauthorized use or disclosure of Confidential Information following the Chain of Command or directly to the Regional Compliance and Privacy Officer. Reports may also be made to the IASIS Chief Privacy/Information Security Officer at 615-467-1283 or to the IASIS Alert Line at 1-877-898-6080.
3. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
4. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.
5. I agree to cooperate with any investigation by Secretary of the U.S. Department of Health and Human Services(HHS) or any agent or employee of HHS or other oversight agency for the purpose of determining compliance with federal or state privacy and/or security laws.

Protecting Confidential Information

6. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
7. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
8. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards and Company record retention policy.
9. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
10. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.

11. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Company using email or other electronic communication methods, I will ensure that the Information is encrypted according to Company Information Security Standards.
12. I may not remove Confidential Information from the Company premises without appropriate authorization. When authorized to remove Confidential Information I acknowledge that I am responsible for securing, protecting from disclosure to others, and ensuring its return to the Company. If instructed I will ensure destruction of the Confidential Information in a manner that renders it unreadable and unusable and document such destruction.

Following Appropriate Access

13. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
14. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

Using Portable Devices and Removable Media

15. I will not copy or store Confidential Information on removable media or portable devices such as personal laptops, cell phones, CDs, thumb drives, external hard drives, etc., unless specifically authorized to do so as part of my job. If I do copy or store Confidential Information on removable media, I will encrypt the information while it is on the media according to Company Information Security Standards.
16. I understand that any mobile device (i.e. cell phone) that synchronizes company data (*e.g.*, Company email) may contain Confidential Information and as a result, must be protected. Because of this, I understand and agree that the Company has the right to:
    a. Require the use of only encryption capable devices.
    b. Prohibit data synchronization to devices that are not encryption capable or do not support the required security controls.
    c. Implement encryption and apply other necessary security controls (such as an access PIN and automatic locking) on any mobile device that synchronizes company data regardless of it being a Company or personally owned device.
    d. Remotely "wipe" any synchronized device that: has been lost, stolen or belongs to a terminated employee or affiliated partner.
    e. Restrict access to any mobile application that poses a security risk to the Company network.

Doing My Part – Personal Security

17. I understand that I will be assigned a unique identifier to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
18. I will:
    a. Use only my officially assigned User-ID and password.
    b. Use only approved licensed software.
    c. Use a device with virus protection software.
19. I will never:
    a. Disclose passwords, PINs, or access codes.
    b. Use tools or techniques to break/exploit security measures.
    c. Connect unauthorized systems or devices to the Company network.
20. I will practice good workstation security measures such as locking the device when unattended and positioning screens away from public view.
21. I will immediately notify my manager, Facility Information Security Official (FISO) or help desk if:

a. my password has been seen, disclosed, or otherwise compromised;
b. media with Confidential Information stored on it has been lost or stolen;
c. I suspect a virus infection on any system;
d. I am aware of any activity that violates this agreement, privacy and security policies; or
e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

22. I will read the policies and procedures as they relate to my job responsibilities, will complete the training courses required by the Company, and shall abide by the Company's policies and procedures that govern Confidential Information.

Upon Termination

23. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
24. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
25. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above. I understand that nothing in this Agreement prevents me from using or disclosing Confidential Information when required by law.

Employee/Workforce Member Signature	Facility Name	Date
Employee/Workforce Member Printed Name	Email	Phone
Business Entity Name	Business Entity Phone	

ATTACHMENT B

IASIS Provider Confidentiality and Security Agreement

Note: this form is for non-employed physicians, providers and their non-IASIS-employed staff

I understand that the IASIS affiliated facility or business entity (the "Company") at which I have manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my affiliation with the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company provided systems.

General Rules

1. I will act in accordance with the Company's Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.
4. I have no intention of varying the volume or value of referrals I make to the Company in exchange for Internet access service or for access to any other Company information.
5. I have not agreed, in writing or otherwise, to accept Internet access in exchange for the referral to the Company of any patients or other business.
6. I understand that the Company may decide at any time without notice to no longer provide access to any systems to physicians on the medical staff unless other contracts or agreements state otherwise. I understand that if I am no longer a member of the facility's medical staff, I may no longer use the facility's equipment to access the Internet.

Protecting Confidential Information

7. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information off Company property unless specifically authorized to do so as part of my job.
8. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
9. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards.
10. In the course of treating patients on Company property, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
11. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
12. I will secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with industry-approved security standards, such as encryption.

Following Appropriate Access

13. I will only access or use systems or devices I am officially authorized to access, will only do so for the purpose of delivery of medical services at this facility, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
14. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

Credentialed Medical Staff Responsibilities

15. I will insure that only appropriate personnel in my office, who have been through a screening process, will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
16. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.
17. I agree that if I, or my staff, stores Confidential Information on non-Company media or devices (*e.g.*, PDAs, laptops) or transmits data outside of the Company network, that the data then becomes my sole responsibility to protect according to federal regulations, and I will take full accountability for any data loss or breach.
18. I will ensure that members of my office staff use a unique identifier to access Confidential Information.

Doing My Part – Personal Security

19. I understand that I will be assigned a unique identifier to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
20. I will:
    a. Use only my officially assigned User-ID and password (and/or token (*e.g.*, SecurID card)).
    b. Use only approved licensed software.
    c. Use a device with virus protection software.
21. I will never:
    a. Disclose passwords, PINs, or access codes.
    b. Use tools or techniques to break/exploit security measures.
    c. Connect unauthorized systems or devices to the Company network.
22. When using Company workstations I will practice security measures such as locking the screen when not in use and positioning screens away from public view.
23. I will immediately notify the Company Facility Information Security Officer (FISO), or help desk if:
    a. my password has been seen, disclosed, or otherwise compromised
    b. media with Confidential Information stored on it has been lost or stolen;
    c. I suspect a virus infection on any system;
    d. I am aware of any activity that violates this agreement, privacy and security policies; or
    e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

24. I agree to notify the facility Medical Staff Office within 24 hours, or the next business day, when members of my office staff are terminated, so that user accounts to Company systems are appropriately disabled in accordance with Company standards.
25. I agree that my obligations under this Agreement will continue after termination of my privileges, expiration of my contract, or my relationship ceases with the Company.

26. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
27. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Provider/Staff Signature		Date
Provider/ Staff Printed Name	Email	Phone
Clinic Name:		
Clinic Address		Phone

ATTACHMENT C

IASIS Provider Confidentiality and Security Agreement

Note: this form is for external entities, vendors and their staff

I understand that the IASIS affiliated facility or business entity (the "Company") at which I have manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my affiliation with the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company provided systems.

General Rules

1. I will act in accordance with the Company's Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.
4. I understand that the Company may decide at any time without notice to no longer provide access to any systems to external entities, vendors and their staff unless other contracts or agreements state otherwise. I understand that when my contract ends, I may no longer use the facility's equipment to access the Internet.

Protecting Confidential Information

5. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information off Company property unless specifically authorized to do so as part of my job.
6. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
7. I will not in any way divulge copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards.
8. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
9. I will secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with industry-approved security standards, such as encryption.

Following Appropriate Access

10. I will only access or use systems or devices I am officially authorized to access, will only do so for the purpose of delivery of contractual obligations, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.

External Entity and Vendor Responsibilities

11. I will insure that only appropriate personnel, who have been through a screening process, will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
12. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.

13. I agree that if I, or my staff, stores Confidential Information on non-Company media or devices (*e.g.*, PDAs, laptops) or transmits data outside of the Company network, that the data then becomes my sole responsibility to protect according to federal regulations, and I will take full accountability for any data loss or breach.
14. I will ensure that members of my office staff use a unique identifier to access Confidential Information.

Doing My Part – Personal Security

15. I understand that I will be assigned a unique identifier to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
16. I will:
    d. Use only my officially assigned User-ID and password (and/or token (*e.g.*, SecurID card)).
    e. Use only approved licensed software.
    f. Use a device with virus protection software.
17. I will never:
    d. Disclose passwords, PINs, or access codes.
    e. Use tools or techniques to break/exploit security measures.
    f. Connect unauthorized systems or devices to the Company network.
18. When using Company workstations I will practice security measures such as locking the screen when not in use and positioning screens away from public view.
19. I will immediately notify the Company Facility Information Security Officer (FISO), or help desk if:
    f. my password has been seen, disclosed, or otherwise compromised
    g. media with Confidential Information stored on it has been lost or stolen;
    h. I suspect a virus infection on any system;
    i. I am aware of any activity that violates this agreement, privacy and security policies; or
    j. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

20. I agree to notify the facility FISO within 24 hours, or the next business day, when members of my staff are terminated, so that user accounts to Company systems are appropriately disabled in accordance with Company standards.
21. I agree that my obligations under this Agreement will continue after expiration of my contract, or my relationship ceases with the Company.
22. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
23. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

External Entity or Vendor/Staff Signature		Date
External Entity or Vendor/ Staff Printed Name	Email	Phone
External Entity or Vendor Name:		
External Entity or Vendor Address		Phone