Cyber Security Policy

Aspermont Small Business Development Center, Inc.

Approved ____

Board President ____

The purpose of this cybersecurity policy is to safeguard ASBDC's valuable information assets, such as data and systems, from cyber threats and attacks. It outlines the rules, standards, and procedures that guide individuals within the organization in protecting these assets, ensuring compliance with relevant regulations, and fostering a strong security culture.

CTSI, ASBDC's information technology company, takes care of the biggest part of the security for our system. They monitor the system for malware and other cyber issues, backup the system regularly, and provide updates as needed. They are always available to the staff for any problems that arise.

CTSI has set up the company's network to be secure and only accessible by staff of the company. We do have a guest account set up for visitors to our facility to only access the internet.

CTSI provides all staff members with cybersecurity training—annual and weekly training videos. CTSI also provide the company with an annual risk assessment.

Table of Contents

Security Policy #1

Written Information Security Policy (WISP)

Statement of Policy

The objective of Aspermont Small Business Development Center (ASBDC) ("The Company") in the development and implementation of this comprehensive written information security policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personally identifiable information (PII) of customers, clients and employees as well as sensitive company information that could harmful if unauthorized access were to occur. The WISP sets forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and sensitive company information.

The use of the term ***employees*** *will include all of The Company's owners, managers, employees, all independent contractors and temporary employees.*

Purpose of Policy

The purpose of the WISP is to better:

1) Ensure the security and confidentiality of **personally identifiable information (PII)** of customers, clients, employees or vendors as well as **sensitive company data** which includes emails, confidential company information (i.e. company expansion plans, manufacturing processes, highly secretive information, etc.), employee information and the like.;

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and

3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud or harm to The Company.

Scope of Policy

In formulating and implementing the WISP, The Company has addressed and incorporated the following protocols:

1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII and sensitive company data.

2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII and sensitive company data.

3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risk.

4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.

5) Implemented regular monitoring of the effectiveness of those safeguards.

Security Safeguards

The follow safeguards are effective immediately. The goal of implementing these safeguards are to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII or sensitive company data.

<u>Administrative Safeguards</u>

1) **Security Officer** - The Company has designated the ASBDC Executive Director to implement, supervise and maintain the WISP. This designated employee (the "Security Officer") will be responsible for the following:

    (a) Implementation of the WISP including all provisions outlined in **Security Safeguards.**

    (b) Training of all employees that may have access to PII and sensitive company data. Employees should receive annual training and new employees should be trained as part of the new employee hire process.

    (c) Regular monitoring of the WISP's safeguards and ensuring that employees are complying with the appropriate safeguards.

    (d) Evaluating the ability of any Third Party Service Providers to implement and maintain appropriate security measures for the PII and sensitive company data to which The Company has permitted access, and requiring Third Party Service Providers, by contract, to implement and maintain appropriate security measures.

(e) Reviewing all security measures at least annually, or whenever there is a material change in The Company's business practices that may put PII and sensitive company data at risk.

(f) Investigating, reviewing and responding to all security incidents or suspected security incidents.

2) **Security Management** - All security measures will be reviewed at least annually, or whenever there is a material change in The Company's business practices that may put PII or sensitive company data at risk. This should include performing a security risk assessment, documenting the results and implementing the recommendations of the security risk assessment to better protect PII and sensitive company data. The Security Officer will be responsible for this review and will communicate to management the results of that review and any recommendations for improved security arising out of that review.

3) **Minimal Data Collection -** The Company will only collect PII of clients, customers or employees that is necessary to accomplish legitimate business transactions or to comply with any and all federal, state or local regulations.

4) **Information Access** - Access to records containing PII and/or sensitive company data shall be limited to those persons whose job functions requires a legitimate need to access the records. Access to the records will only be for a legitimate job-related purpose. In addition, pre-employment screening should take place to protect PII and sensitive company data.

5) **Employee Termination -** Terminated employees must return all records containing PII and sensitive company data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.). A terminated employee's physical and electronic access to PII and sensitive company data must be immediately blocked. A terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to The Company's premises or information. A terminated employee's remote electronic access to PII and sensitive company data must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. **See Security Policy #2 – Termination Policy.**

6) **Security Training** – All employees, which includes all owners, managers, employees, all independent contractors and temporary employees that may have access to PII and sensitive company data, will receive security training . Employees should receive at least annual training and new employees should be trained as part of the new employee hire

process. Employees should be required to show their knowledge of the information and be required to pass an exam that demonstrates their knowledge. Documentation of employee training should be kept and reviewed.

7) **WISP Distribution -** A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing or electronically, that he/she has received a copy of the WISP and will abide by its provisions. **See Security Policy #1 - Written Information Security Policy (WISP) Appendix A – WISP Employee Acknowledgement Form.**

8) **Contingency Planning** – All systems that store PII and/or sensitive company data should have the data backed up on, at least, a nightly basis. Data should be encrypted and be stored offsite. Disaster Recovery mechanisms and documented procedures should be in place to restore access to PII and sensitive company data as well as any operational systems that The Company relies on. A system criticality assessment should be performed that defines how critical each of The Company's systems are. Systems that are critical to operations should be restored before non-critical systems. On a periodic basic, data backups, data restoration and Disaster Recovery procedures should be tested and validated. **See Disaster Recovery Template.**

9) **Security Incident Procedures** - Employees are required to report suspicious or unauthorized use of PII and/or sensitive company data to a supervisor or the Security Officer. Whenever there is an incident that requires notification pursuant to any federal or state regulations, the Security Officer will conduct a mandatory post-incident review of the events and actions taken in order to determine how to alter security practices to better safeguard PII and sensitive data. **See Security Policy #3- Security Incident Response.**

10) **Emergency Operations** – Procedures should be in place to define how The Company will respond to emergencies. Procedures should include employee contact information, critical vendor contact information, important vendor account information as well as any emergency operating procedures. **See Emergency Operations Template.**

11) **Data Sensitivity Classification** – All data that The Company stores or accesses should be categorized in terms of the sensitive nature of the information. For example, PII and sensitive company data might have a very high sensitivity and should be highly protected. Whereas publicly accessible information might have a low sensitivity and requires minimal protection.

12) **Third Party Service Providers** - Any service provider or individual ("Third Party Service Provider") that receives, stores, maintains, processes, or otherwise is permitted access to any file containing PII and/or sensitive company data shall be required to protect PII and sensitive company data. The Third Party Service Providers must sign service agreements that

contractually hold them responsible for protecting The Company's data. Examples include third parties who provide off-site backup of electronic data; website hosting companies; credit card processing companies; paper record copying or storage providers; IT / Technology Support vendors; contractors or vendors working with customers and having authorized access to PII and/or sensitive company data.

13) **Sanctions** - All employment contracts, where applicable, should be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of PII and/or sensitive company data as defined by the WISP. Disciplinary actions will be taken for violations of security provisions of the WISP (The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the PII and/or sensitive company data affected by the violation). **See Security Policy #4 – Sanction Policy.**

14) **Bring Your Own Device (BYOD) Policy** – The Company may allow employees to utilize personally owned devices such as laptops, smartphones and tablets. If staff uses their personal devices, they will use the guest account to access only the internet on these devices. These devices will not be able to access the company network where Pii is stored.

Physical Safeguards

15) **Facility Access Controls** – The Company will implement physical safeguards to protect PII and sensitive company data. There will be physical security on facilities / office buildings to prevent unauthorized access. All systems that access or store PII and/or sensitive company data will be physically locked. Employees will be required to maintain a "clean desk" and ensure that PII and/or sensitive company data is properly secured when they are not at their desk. The Security Officer will maintain a list of lock combinations, passcodes, keys, etc. and which employees that have access to the facilities and PII and/or sensitive data. Visitors will be restricted from areas that contain PII and/or sensitive company data. **See Security Policy #10 - Facility Security Plan.**

16) **Network Security** – The Company will implement security safeguards to protect PII and sensitive company data. Safeguards include; isolating systems that access or store PII and/or sensitive company data, the use of encryption on all portable devices, physical protection on portable devices, ensuring that all systems run up-to-date anti-malware, implementing network firewalls, performing periodic vulnerability scans, capturing and retaining network log files as well as ensuring that servers and critical network equipment are stored in an environmentally safe location. **See Security Policy #5 – Network Security**

Technical Safeguards

17) **Access Control** - Access to PII and sensitive company data shall be restricted to approved active users and active user accounts only. Employees will be assigned unique user accounts and passwords. Systems containing PII and sensitive company data should have automatic logoff procedures to prevent unauthorized access. **See Security Policy #6 – Access Control**

18) **Computer Use** – All employees will be given a Computer Use Policy that defines acceptable and unacceptable use of The Company's computing resources. Employees should be required to sign the Computer Use Policy to acknowledge acceptance of the policy. **See Security Policy #7 – Computer Use**

19) **Data Disposal** - Written and electronic records containing PII and sensitive company data shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. **See Security Policy #8 – Equipment Disposal**

20) **System Activity Review** - All systems that store or access PII and sensitive company data should utilize a mechanism to log and store system activity. Periodic system activity reviews should occur and identify unauthorized access to PII and sensitive company data. Any unauthorized access should be reported to the Data Security Coordinator. **See Security Policy #3- Security Incident Response**

21) **Encryption** - To the extent technically feasible all portable devices that contain PII and sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

Security Policy #2

Termination Policy

Purpose of Policy

This policy defines the steps required to revoke both physical and system access to The Company's facilities and network resources.

Termination of Access: it is essential that supervisors and/or Information Technology (IT) terminate access to company facilities and systems in a timely manner to protect the information, systems and resources. Supervisors / IT are required to terminate access immediately upon termination (or even before when possible) of the employee, workforce member or contractor.

1) A terminated employee shall be required to surrender all keys, IDs, access cards/codes or badges, business cards, parking permits and the like, that permit access to The Company's premises or information.

2) A terminated employee's physical and electronic access to PII and sensitive company data must be immediately blocked.

3) A terminated employees must return all records containing PII and sensitive company data, in any form, that may be in the former employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).

4) Revoke all computer, network, and data access the terminated employee has for both internal and external systems:

    1) Internal systems

    1. Microsoft Windows / Network Domain
    2. Systems that store or access PII and sensitive company data
    3. Email
    4. Database applications
    5. Any other systems that the terminated employee has access to

    2) External systems

    1. Cloud based systems such as credit card processing systems, billing systems, customer relationship management (CRM), etc.

5) Remote access should be removed

6) Wireless access should be removed

All termination steps that are taken should be documented and retained for legal purposes and/or federal or state regulations.

Security Policy #3

Security Incident Procedures

Purpose of Policy

The purpose of the policy is to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

It should be noted that breach definitions, remediation steps and breach notification steps vary between various federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), The Gramm-Leach-Bliley Act (GLB Act or GLBA) and other federal regulations. In addition, most state regulated breach laws vary between individual states. In is highly recommended to consult with breach experts or legal counsel to determine The Company's responsibilities.

Definitions

Breach

Breach means the acquisition, access, use, or disclosure of personally identifiable information (PII) or sensitive company data such as email, employee information, confidential information, etc. which compromises the security or privacy of the PII or sensitive company data.

Unsecured PII

Unsecured PII means PII that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology such as encryption. The definition of unsecured PII varies between different federal and state regulations.

Reporting and Response

The Company will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of PII and sensitive company data will be reported and responded to.

The Company shall have a Security Incident Response Team (SIRT) charged with the responsibility of identifying, evaluating and responding to security incidents. The Privacy Security Officer shall oversee the activities of the SIRT.

The SIRT will be responsible for investigating all known or suspected privacy and security incidents.

The SIRT will document a procedure for all employees to follow to report privacy and security incidents. See Appendix A – Security Incident Response Log or the Security Incidents Module in the Security Portal.

The Company will ensure that all employees receive training on how to identify and report security incidents.

All employees must follow the documented procedure to report security incidents. In addition, employees must report all known or suspected security incidents.

All employees must assist the SIRT with any security incident investigations.

Breach Determination

The Security Incident Response Team (SIRT) will investigate all reported and suspected security breaches. The SIRT will refer to federal or state regulations to help with breach determination. Breach determination varies between federal regulations such as HIPAA and GLBA. In addition, breach determination varies significantly between state regulations (for example, what may be considered a breach in one state may not be a breach in another state).

Breach Notification

If the SIRT determines that a breach of unsecured PII has occurred, breach notification of affected individuals may be required. The SIRT will refer to federal or state regulations to help with breach notification requirements. Breach notification requirements varies between federal regulations such as HIPAA and GLBA. In addition, breach notification requirements varies significantly between state regulations (for example, one state may have breach notification requirements that varies significantly from breach notification requirements in another state).

Key elements of a breach notification include:

Date of discovery--Usually a breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

Timeliness of notification--The Company will provide the required notifications without unreasonable delay after discovery of a breach. The amount of time The Company has to notify affected individuals varies between federal and state regulations.

Content of notification--If required, a notification will be provided to each individual affected by the discovered breach. The notification should include the following:

A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

A description of the types of unsecured PII that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number or other types of information were involved);

Any steps individuals should take to protect themselves from potential harm resulting from the breach;

A brief description of what The Company is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

Contact procedures for individuals to ask questions or learn additional information, which should include a telephone number, an e-mail address, Web site, or postal address.

The notification should be written in plain language.

Methods of notification

The following methods are usually used to notify individuals affected by the discovered breach:

Written notice--Written notification by first-class mail to the individual at the last known address of the individual or, via e-mail if the individual agrees to e-mail notice. The notification may be provided in one or more mailings as information is available. If the individual is deceased notifications are usually sent to next of kin or personal representative

Substitute notice--If contact information is out of date and written notification cannot be made, a substitute notification may be used. A substitute notification usually in the form of either a conspicuous posting on The Company's home page of its Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice should include a contact phone number.

Notification to media--In addition to notifying individuals of a known breach, a notification to the media may be required as well.

Notification to federal or state regulatory agencies--The Company may need to report breaches of unsecured information to federal or state regulatory agencies.

Notification by Third Party Service Providers--Third Party Service Provider responsible for a breach of The Company's PII or sensitive company data should be required to notify The Company within a pre-determined reasonable timeframe. The timeframe should be defined in a Service Provider Agreement. Third Party Service Provider breaches may result in The Company having to notify The Company's affected individuals (such as customers, employees, etc.).

Security Policy #4

Sanction Policy

Scope of Policy

This policy governs employee Sanctions and disciplinary actions for The Company. All employees must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every employee.

Policy Statement

- It is the Policy of The Company to establish and implement appropriate, fair and consistent sanctions for employees who fail to follow established policies and procedures, or who commit various offenses.
- Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
- All employee Sanctions will be documented

Based on the severity of the violation, develop varying levels of disciplinary action such as:

- Verbal warning
- Written warning
- Education – training/retraining
- Removal of system privileges
- Suspension without pay
- Termination of employment

Procedures

- Inadvertent release of PII and sensitive company data will investigated and the punishment will be determined by management and the extent of harm to individual involved.
- Employees accessing PII and sensitive company data files that they do not have a reason to access is a violation that may result in immediate termination.
- Blatant disregard for The Company's Policies and Procedures may result in immediate termination.
- Intentional release of PII and sensitive company data to someone who should not have access to the information WILL result in immediate termination and possible prosecution.

Security Policy #5

Network Security

Purpose of Policy

The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII and sensitive company data to ensure that appropriate security is maintained and that access is restricted to authorized employees.

Network Security

The Company will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices including laptops, smartphones, CD-ROMs, DVDs, USB Drives, etc. that store or access PII and sensitive company data.

1) Workstations and laptops that are in common areas that store or access PII and/or sensitive company data should be physically placed with the monitor so that it prohibits unauthorized people from viewing confidential information such as logins, passwords, PII and/or sensitive company data.

2) Workstations and laptops that are in common areas that store or access PII and sensitive company data should utilize privacy screens to prevent unauthorized access to the data.

3) Workstations and laptops that are in common areas that store or access PII and sensitive company data should be secured by restraints such as locking cables.

4) To the extent technically feasible all portable devices that contain PII and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and/or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

5) Portable devices and media should be concealed from view when offsite to prevent theft.

6) All network servers, application servers, routers, database systems, device management system hardware, and other servers should be located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.

7) All workstations, servers and portable devices will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions. Employees must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Employees must not disable these tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.

8) A network firewall should be in place to protect PII and/or sensitive company data. The firewall protection should be up to date. Firewalls should be monitored and alerts should be triggered in the event of unauthorized intrusion or suspected intrusion.

9) Log files from network equipment should be stored and retained. Log files from network equipment include; firewalls, network servers, desktops, laptops and other devices. The required length of retention of log files may vary depending on federal, state or industry regulations.

10) All workstations, servers and portable devices, where feasible, must implement a security patch and update procedure to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

11) Periodic network vulnerability scans should be performed on all internal as well as external (Internet facing servers, websites, etc.) systems. Results of the vulnerability scans should be analyzed and known vulnerabilities should be remediated and/or patched. After all vulnerabilities are remediated, an external network penetration test should be performed to ensure that unauthorized external access into the network is prevented.

12) Reasonable and appropriate steps will be taken to prevent unauthorized access to workstations, servers and portable devices from misuse and physical damage, vandalism, power surges, electrostatic discharge, magnetic fields, water, overheating and other physical threats.

    a. Workstations must not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions should also be taken to ensure that workstations cannot be affected by problems caused by utilities, such as water, sewer and/or steam lines that pass through the facility.

    b. All facilities that store systems that contain PII and/or sensitive company data, should have appropriate smoke and/or fire detection devices, sprinklers or other approved fire suppression systems, and working fire extinguishers in easily accessible locations throughout the facility.

    c. All servers that contain PII and/or sensitive company data, should be connected to an Uninterrupted Power Supply (UPS) to prevent server crashes during power outages or spikes. Servers should be configured to shut down in a controlled manner if the power outage is for an extended period of time.

    d. All systems should be connected to surge protectors, where feasible, to protect against power spikes and surges.

13) A user identification and password authentication mechanism shall be implemented to control user access to the system. (See Security Policy #6 - Access Control).

14) Employees who suspect any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to the Security Officer.

Security Policy #6

Access Control

Purpose of Policy

The purpose of the policy is to assure that systems containing PII and/or sensitive company data are accessed only by those persons or software programs that have been granted appropriate access rights

Unique User Identification

1) Employees will be assigned a unique user identification (i.e. userid) in order to access any system or application that transmits, receives or stores PII and/or sensitive company data.

2) Each employee must ensure that their assigned user identification is appropriately protected and only used for legitimate access to systems or applications.

3) If an employee believes their user identification has been comprised, they must report the security incident.

4) Employees should be aware of the following password procedures to create and use strong passwords to protect PII and sensitive company data:

    a. Should be a minimum of eight characters in length.

    b. Should incorporate both upper and lower case letters (e.g. a-z and A-Z)

    c. Should incorporate digits and punctuation characters as well as letters e.g., 0-9, (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; " ' | \ / ? < > , . ~ `)

    d. Should not be words found in a Dictionary.

    e. Should not include easily guessed information such as personal information, names, pets, birth dates, etc.

5) Employees should be aware of the following procedures to protect passwords:

    a. Passwords should not be written down

    b. Passwords should not be shared with other employees

   c. If an employee suspects that their password has been compromised they should report the incident immediately

6) Passwords should be changed at least every 90 days

7) After a number of failed password attempts, the employee's account should be disabled (e.g. 3 or 5 failed attempts)

Automatic Logoff

1) Systems that access or store PII and/or sensitive company data should implement an automatic logoff after a determined period of inactivity (i.e. 10 minutes of inactivity). Employees would need to login again to regain access and continue the session.

2) When leaving a server, workstation, or other computer system unattended, employees must lock or activate the system's automatic logoff mechanism (e.g. CTRL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing or accessing PII and/or sensitive company data.

Encryption and Decryption

22) To the extent technically feasible all portable devices that contain PII and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

23) Employees should be trained on the use of encryption to protect PII and sensitive company data.

24) All backup tapes and media that contain PII and/or sensitive company data should utilize encryption to protect the data.

25) Secure encrypted remote access procedures should be implemented to protect systems that access or store PII and/or sensitive company data.

    a. Authentication and encryption mechanisms should be required for all remote access sessions to networks containing PII and/or sensitive company data. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and encrypted Citrix/RDP client access.

    b. Two-factor authentication (i.e. SMS pin notification) should be implemented where technically feasible.

26) All wireless access to networks should utilize encryption mechanisms.

    a. Employees should not utilize open public Wi-Fi networks

Security Policy #7

Computer Use

Purpose of Policy

The purpose of this policy is to ensure that employees understand what functions should and should not be performed on The Company's computers and network to maximize the security of PII and sensitive company data. The policy also provides guidance regarding proper safeguards of PII and sensitive company data when accessing social media sites.

Computer Use

1) To ensure that workstations and other computer systems that may be used to send, receive, store or access PII and sensitive company data are only used in a secure and legitimate manner, all employees must comply with The Company's Computer Use Policy, a copy of which is attached as Appendix A.

2) The Company may provide workstations and other computer systems to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy.

3) The Company may remove or deactivate any employee's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

4) Employees must be assigned and use a unique User Identification and Password (**See Security Policy #6 - Access Control**)

5) Employees that use The Company's information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, The Company may log, review, or monitor any data stored or transmitted on its information system assets.

Computer Use

Introduction

This document provides guidelines for appropriate use of computer facilities and services. It is not a comprehensive document covering all aspects of computer use. It offers principles to help guide employees, and specific policy statements serve as a reference point. It will be modified as new questions and situations arise.

Computers, the Internet and electronic mail (e-mail) are powerful research, communication, commerce and time-saving tools that are made available to employees. The use of this efficient and effective communication tool is critical but, like any tools, computers, the Internet and e-mail have the potential to be used for inappropriate purposes.

Workstations and other computer systems may be provided to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy.

Policy

The following policies on computer, the Internet and electronic mail usage shall be observed by all employees.

- Users of the Internet and e-mail are to comply with all appropriate laws, regulations and generally accepted Internet etiquette.
- Primary purpose of the Internet and e-mail is to conduct official business.
- Users should identify themselves properly when using the Internet and e-mail, conduct themselves professionally, and be aware that their activities reflect on the reputation and integrity of all our employees.
- Each user is individually responsible for the content of any communication sent over or placed on the Internet and e-mail.
- All employees have a responsibility to ensure a respectful workplace. Computer equipment must not be used to visit Internet sites that contain pornographic or sexually explicit information, pictures, or cartoons.
- Exceptions to this policy are only allowed when pre-approved by supervisors or company management and deemed necessary for official business, research or investigatory work.

The following actions are prohibited. It is unacceptable for employees to:

- Knowingly or intentionally publish, display, transmit, retrieve or store inappropriate or offensive material on any department computer system.
- Create or distribute defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material.

- View or distribute obscene, pornographic, profane, or sexually oriented material.
- Violate laws, rules, and regulations prohibiting sexual harassment.
- Engage in any unauthorized activities for personal financial gain.
- Place advertisements for commercial enterprises, including but not limited to, goods, services or property.
- Download, disseminate, store or print materials including articles and software, in violation of copyright laws.
- Download any software, including but not limited to games, screen savers, toolbars or any other browsing tools without the permission of supervisors, company management or IT staff.
- Violate or infringe on the rights of others.
- Conduct business unauthorized by the company.
- Restrict or inhibit other users from using the system or the efficiency of the computer systems.
- Cause congestion or disruption of networks or systems, including distribution of chain letters.
- Transmit incendiary statements, which might incite violence or describe or promote the use of weapons.
- Use the system for any illegal purpose or contrary to company policy or business interests.
- Connect a personal computer to the company network without having the computer checked by IT staff to insure no threatening viruses / programs infect the company network.
- Monitor or intercept the files or electronic communications of other employees or third parties.
- Hack or obtain access to systems or accounts they are not authorized to use.
- To disclose a Login ID(s) or password to anyone nor allow anyone to access any information system with someone else’s Login ID(s) or passwords
- Use other people's Login ID(s) or passwords to access any information system for any reason.
- To post any PII or sensitive company data on social network sites, public forums, etc. This includes posting pictures of PII or sensitive company data or pictures of customers without permission.
- Employees shall not remove electronic media that contains PII or confidential or proprietary information unless such removal is authorized by an employee’s supervisor or company management.

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

Employees will immediately report any activity that violates this agreement to the employee's supervisor, company management or company Security Officer.

Security Policy #8

Disposal Procedure

Purpose of Policy

All media containing PII and sensitive company data, will be disposed of in a manner that destroys the data and does not allow unauthorized access to the data.

Procedures for computer/hardware disposal

The Security Officer or delegate will notify the Information Technology (IT) department/company/individual of equipment that needs to be disposed of.

1) The Security Officer or delegate will determine data sensitivity of data to be disposed of. (See Data Classification Table below)

2) IT will assess the condition of the equipment, and:
   a. IT will track the disposal of the device (type of hardware, serial number, etc). See Appendix A: Media Disposal Log
   b. IT will run approved wiping software on all devices to make sure all PII and sensitive company data is removed from the device.
      i. This may include physical destruction (See Methods of Destruction below)
   c. IT will verify the hardware's data has been removed.
   d. IT will dispose of the hardware.

3) The Security Officer or delegate / IT will document the destruction of the asset and keep a record. See Appendix A: Media Disposal Log.

4) If taken to outside facility - The media shall be taken to an approved, certified facility for erasure or destruction. A letter of certification regarding date and time of erasure/destruction shall be obtained.

Data Classification Table:

1) **Low (Unclassified)** - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
    - Basic operating system, personal files, etc.

2) **Med (Sensitive but not Confidential)** - Erase the data using any means such as reformatting or degaussing.
    - This would be for business related information which is not considered sensitive company data.

3) **High (Confidential)** - The data must be erased using an approved technology to make sure it is not readable using special technology techniques. (See method of destruction below)
    - This would be for PII and sensitive company data.

Examples of hardware devices include:

- Workstation
- Laptop
- Tablet (iPad/Android)
- Smartphones
- Server hard drives
- Memory stick (USB drives)
- CD ROM disk / DVD ROM
- Storage / Backup tape(s)
- Hard drives
- Copiers / Scanners / Fax machines
- Any equipment that contains PII or sensitive company data

Security Policy #9

Facility Security Plan

Purpose of Policy

The purpose of the policy is to define the procedures that will limit physical access to PII and sensitive company data and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

Facility Security Plan

1) Physical security of office buildings must be implemented to protect PII and sensitive data as well as other company assets. Physical measures might include: alarm systems, surveillance camera, fences, locked gates / doors, etc.

2) All systems that store or access PII and/or sensitive company data should be stored in locked rooms, closets or cabinets to prevent unauthorized access. Access to these facilities should be minimized and limited to only employees and/or vendors that need access to perform their job function.

3) Where practical, all visitors should be restricted from areas where files or systems containing PII and/or sensitive company data are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files or systems containing PII and/or sensitive company data are stored.

4) The Security Officer shall maintain a secured and confidential master list of all lock combinations, passcodes, and keys. The list will identify which employee possess keys, keycards, or other access devices and that only approved employees have been provided access credentials.

Appendix A – Cybersecurity Policy Employee Acknowledgement Form

I have read, understand, and agree to comply with the ASBDC Cybersecurity Policy), rules, and conditions governing the security of PII and sensitive company data. I am aware that violations of the policy may subject me to disciplinary action and may include termination of my employment.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

______________________________	______________________
Signature	Date
______________________________	______________________
Employee's Supervisor Signature	Date

Appendix B – Security Incident Response Log

Incident Identification Information	
Name:	
Phone:	
Email:	
Date/Time Detected:	
System / Application Affected:	
Incident Summary	
Type of Incident Detected: (Denial of Service, Malicious Code, Unauthorized Access, Unauthorized Use / Disclosure, Unplanned System Downtime, Other)	
Description of Incident:	
Names of Others Involved:	
Incident Notification	
How Was This Notified? (Security Office, IT Personnel, Human Resources, Other)	
Response Actions Include Start and Stop times	
Identification Measures (Incident Verified, Accessed, Options Evaluated):	
Containment Measures:	
Evidence Collected (Systems Logs, etc.):	

Appendix C
Disaster Recovery Plan

Introduction

ASBDC has adopted this Disaster Recovery Policy. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

Scope of Policy

The scope of this disaster recovery plan addresses technical recovery only in the event of a significant disruption. All personnel of ASBDC must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce. The disaster recovery plan should be tested annually to maintain its integrity.

Considerations

- A disaster may occur at any time, not necessarily during work
- ASBDC should establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing PII / sensitive data
- hours
- Systems that contain PII / sensitive data can be affected or destroyed in many ways, such as:
- Flooding
- Fire
- Loss of power
- Acts of God: Tornado, tsunami or hurricane
- Hackers
- Unauthorized access or malicious activity

Policy Statement

It is the policy of ASBDC to establish and implement processes and procedures to create and maintain retrievable exact copies of PII / sensitive data.

Disaster Recovery Procedures

Phase 1 - Response

- Contact required personnel (identify team members/roles that will be needed for recovery)
- Determine recovery strategies/options to be taken based on disaster

Phase 2 – Recovery

- Implement recovery procedures/failover
  - Identify restoration procedures
  - Assess risk for each procedure

    - Implement procedures

Phase 3 – Validation

- Validate integrity of restored data and the accessibility of that data
    - Test the recovery and communicate to organization

Pre-disaster measures

- Backup all PII / sensitive data with accordance to ASBDC's backup policy
- Test integrity of backups (no less than bi-weekly or monthly)
- Protect by uninterruptible power supplies (UPS) all servers and other critical equipment from damage in the event of an electrical outage
- Training in disaster preparation and recovery, and knowledge of responsibilities in the event of a disaster (share Emergency Operations Plan with employees)

Disaster Recovery Teams and Responsibilities

In the event of a disaster, different groups will be required to assist in the effort to restore normal functionality to the employees of ASBDC.

The different groups and their responsibilities could include:

- *Disaster Recovery Lead(s)—Executive Director*
    - *Manage all processes of the disaster recovery plan*
- *Disaster Recovery Team*
    - *Support the DR lead*
    - *Communicate the disaster to workforce members*
- *IT Department*
    - *Handle all IT related processes of the DR plan*
    - *In the event of a disaster that does not require migration to standby facilities, the team will determine which servers are not functioning at the primary facility*
    - *If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact*
    - *Install and implement any tools, hardware, and systems required for recovery*
- *Management*
    - *Ensure that the Disaster Recovery Team Lead is held accountable for his/her role*
    - *Assist the Disaster Recovery Team Lead in his/her role as required*
- *Finance Department*
    - *Ensure there is sufficient cash on-hand or accessible to deal with small-scale expenses caused by the disaster*
    - *Ensure there is sufficient credit available or accessible to deal with large-scale expenses caused by the disaster. These can include paying for new equipment, repairs for primary facilities, etc.*
    - *Review and approve Disaster Teams' finances and spending*

Disaster Recovery Lead: Executive Director

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs.

Role and Responsibilities

- *Make the determination that a disaster has occurred and trigger the DRP and related processes.*
- *Be the single point of contact for and oversee all of the DR processes.*
- *Determine what systems and processes have been affected by the disaster.*
- *Communicate the disaster to the other disaster recovery teams.*
- *Organize and chair regular meetings of the DR Team leads throughout the disaster.*
- *Create a detailed report of all the steps undertaken in the disaster recovery process*
- *Present to the Management Team on the state of the disaster and the decisions that need to be made.*
- *Organize, supervise and manage all DRP test and author all DRP updates.*
- *Notify the relevant parties once the disaster is over and normal business functionality has been restored.*

Disaster Recovery Team:

Because ASBDC is not a large company, all employee will be a part of the disaster recovery team.

Timeline of Recovery:

Most likely if a disaster occurs, it will affect others in our community. ASBDC will work with others in the community to follow the steps to recovery. Also, the CTSI team will be highly involved in recovery of ASBDC's technology system.

Disaster Recovery Steps

Example:

1. Set the DRP into motion after the Disaster Recovery Lead has declared a disaster
2. Determine the extent of the damage and whether additional equipment/supplies are needed
3. Determine how long it will be before service can be restored, and notify required personnel
4. Replace hardware as necessary to restore service
5. Retrieve and upload backup files if necessary to restore service
6. Ensure that backup procedures are followed
7. Verify the integrity of data restored and the ability for workforce members to access
8. Coordinate activities to ensure that the most critical tasks are being supported as needed
9. Keep administration, information personnel, and others informed of the status of the emergency mode operations
10. Coordinate with administration and others for continuing support and ultimate restoration of normal operations