Clarity Benefit Solutions

Asset Management Policy	Created: 6/16/2021, Updated: 08/31/2024
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 2

Clarity Benefit Solutions is hereinafter referred to as "the company."

1.0 Overview

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

2.0 Purpose

The purpose of this policy is to identify organizational assets and define appropriate protection responsibilities. It includes to ensure that information receives an appropriate level of protection in accordance with its importance to the organization, and to prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

3.0 Scope

The scope of this policy covers all company owned and managed assets including hardware and software.

4.0 Policy

4.1 Inventory of Assets

Assets associated with information and information processing facilities that store, process, or transmit classified information shall be identified and an inventory of these assets shall be drawn up and maintained.

4.2 Ownership of Assets

Assets maintained in the inventory shall be owned by a specific individual or group within the company.

4.3 Acceptable Use of Assets

Rules for the acceptable use of information, assets, and information processing facilities shall be identified and documented in the Information Security Policy.

4.4 Handling of Assets

Employees and users who are issued or handle the company equipment are expected to use reasonable judgment and exercise due care in protecting and maintaining the equipment.

Employees are responsible for ensuring that company equipment is secured and properly attended to whenever it is transported or stored outside of company facilities.

All mobile devices shall be handled in accordance with the Information Security Policy.

4.5 Return of Assets

All employees and third-party users of company equipment shall return all of the organizational assets within their possession upon termination of their employment, contract, or agreement.

5.0 Exceptions

Requests for an exception to this policy must be submitted to the Vice President IT and/or the Executive Team for approval.

6.0 Enforcement

This policy will be enforced by the Vice President IT and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

7.0 Revision History

Revision 1.0, 6/16/2021

Revision 2.0, 1/4/2023

Clarity Benefit Solutions

Clarity Benefit Solutions is hereinafter referred to as "the company."

1.0 Overview

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

2.0 Purpose

The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

3.0 Scope

The scope of this policy covers all company-confidential data, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

4.0 Policy

4.1 Treatment of Confidential Data

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

4.1.1 Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

4.1.2 Transmission

Confidential data must not be 1) transmitted outside the company network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the company's network.

4.1.3 Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.

- Storage media (CD's, DVD's): physical destruction is required.

- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially-available methods for data wiping. Alternatively, the company has the option of physically destroying the storage media.

4.2 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."

- Users must only access confidential data to perform his/her job function.

- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.

- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.

- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.

- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to the company's outsourcing policy for additional guidance.

4.3 Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:

- Strong Encryption. Strong encryption must be used for confidential data transmitted external to the company. If confidential data is stored on laptops or other mobile devices, it must be stored in encrypted form.

- Network Segmentation. Separating confidential data by network segmentation is strongly encouraged.

- Authentication. Strong passwords must be used for access to confidential data.

- Physical Security. Systems that contain confidential data should be reasonably secured.

- Printing. When printing confidential data the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.

- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.

- Emailing. Confidential data must not be emailed outside the company without the use of strong encryption.

- Mailing. If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information.

- Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.

- Confidential data must be removed from documents unless its inclusion is absolutely necessary.

- Confidential data must never be stored on non-company-provided machines (i.e., home

computers).

• If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

4.4 Examples of Confidential Data

The following list is not intended to be exhaustive, but should provide the company with guidelines on what type of information is typically considered confidential. Confidential data can include:

• Employee or customer social security numbers or personal information

• Medical and healthcare information

• Electronic Protected Health Information (EPHI)

• Customer data

• Company financial data (if company is closely held)

• Sales forecasts

• Product and/or service plans, details, and schematics,

• Network diagrams and security configurations

• Communications about corporate legal matters

• Passwords

• Bank account information and routing numbers

• Payroll information

• Credit card information

• Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

4.5 Emergency Access to Data

A procedure for access to confidential and critical data during an emergency must be developed and documented. The company must establish a procedure for emergency access in case the normal mechanism for access to the data becomes unavailable or disabled due to system or network problems.

The procedure should answer the following questions:

- What process must be followed to activate the emergency access procedure?
- What systems will it will involve?
- In what situations should be activated?
- Will it be activated automatically if certain conditions are met, or will it require human intervention? If so, who is authorized to make the decision to implement the procedure?
- Who will be involved in the process and what roles will they perform?

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Authentication A security method used to verify the identity of a user and authorize access to a

system or network.

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Two-Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 5/7/2018

Clarity Benefit Solutions

Data Classification Policy	Created: 5/7/2018, Updated: 08/31/2024
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 5

Clarity Benefit Solutions is hereinafter referred to as "the company."

1.0 Overview

Information assets are assets to the company just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to company operations and the confidentiality of its contents. Once this has been determined, the company can take steps to ensure that data is treated appropriately.

2.0 Purpose

The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

3.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

4.0 Policy

4.1 Data Classification

Data residing on corporate systems must be continually evaluated and classified into the following categories:

1. Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.

2. Public: includes already-released marketing material, commonly known information, etc. There are no requirements for public information.

3. Operational: includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

4. Critical: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

5. Confidential: any information deemed proprietary to the business. See the Confidential Data Policy for more detailed information about how to handle confidential data.

4.2 Data Storage

The following guidelines apply to storage of the different types of company data.

4.2.1 Personal

There are no requirements for personal information.

4.2.2 Public

There are no requirements for public information.

4.2.3 Operational

Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

4.2.4 Critical

Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

4.2.5 Confidential

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

4.3 Data Transmission

The following guidelines apply to transmission of the different types of company data.

4.3.1 Personal

There are no requirements for personal information.

4.3.2 Public

There are no requirements for public information.

4.3.3 Operational

No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

4.3.4 Critical

There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

4.3.5 Confidential

Confidential data must not be 1) transmitted outside the company network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the company's network.

4.4 Data Destruction

The following guidelines apply to the destruction of the different types of company data.

4.4.1 Personal

There are no requirements for personal information.

4.4.2 Public

There are no requirements for public information.

4.4.3 Operational

There are no requirements for the destruction of Operational Data, though shredding is encouraged.

4.4.4 Critical

There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

4.4.5 Confidential

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.

- Storage media (CD's, DVD's): physical destruction is required.

- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially-available methods for data wiping. Alternatively, the company has the option of physically destroying the storage media.

4.5 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Backup To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Two-Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 5/7/2018

Disaster Recovery/Business Continuity Plan

Contents

Revisions

Version	Updated By	Updated On	Comments
1.0	Ron Angelo 10/11/21	10/11/2021	
1.5	Ron Angelo 11/11/21	11/11/2021	
2.0	Ron Angelo 5/11/22	05/11/2022	
3.0	Shailaja Srivastava	01/04/2023	Updated with current Information
4.0	Shailaja Srivastava	08/31/2024	Updated with current Information

Executive Summary

Clarity Benefit Solutions Information Technology (**IT**) group mitigates risks to reduce potential issues and impacts by developing plans that provide the ability to recover from situations including, but not limited to unplanned evacuations; power outages; major water leaks; fire, loss of water/sewer service; severe weather; and any facilities failures that may cause business interruptions.

Plans are designed to account for business interruptions of various lengths and scopes. The plans require that the Information Technology department is able recover critical functions according to their time diagnostics. Each critical function has a designated leader responsible for preparing and testing its recovery script(s). Each critical function also establishes operational guidelines and procedures for disaster recovery to address identified scenarios.

Now is an opportune time to consider the planning, tools and technologies that enable the continuance of operations and reduction in downtime, and logistical back-ups, following a disruption. Cost reducing software, like virtualization, coupled with price reductions in hardware, make implementation easier on budgets. Best of all, if the worst-case scenario becomes front-page news, our business will have a functional and comprehensive business continuity plan. And we will also be prepared with the people, processes, and technology to make it work.

Artifacts

- Key Stakeholders
  - Executive Leadership
  - Senior Staff
- Business
  - Department Leads
    - Will contact clients respectively
- Vendor(s)
  - Two River
  - Liquid Web
  - Salesforce
  - Lenovo
  - Dell
  - InContact

Time to recover matrix per department

Department		
Administrative	Customer Service	Executive
1 day	1-2 Hours	4-8 Hours
Marketing	Payroll	Sales General
2 Day	1-2 Hours	4-8 Hours
Sales National Accounts	Sales- Retail	Sales-Strategic Accounts
4-8 Hours	4-8 Hours	4-8 Hours
Project Management	Finance	Human Resources
1 Day	4-8 Hours	4-8 Hours

Discovery

- Physical Office Locations
  - Clark, NJ (Call Center, Senior Leadership, CRM, Help Desk, Finance)
  - Mesa, AZ (Call Center)
- Assign responsibilities
  - Administrative Steering Committee & Description of Duties
  - Business Continuity Management Team & Description of Duties
  - Support Team
  - Who can declare a disaster & determine level?
  - Communicate/Tree to employees, vendors, and clients
  - Activate Plan
  - Notify Insurance carriers
- Infrastructure Accessibility
- Server Accessibility

Mission Critical Systems/Age/Location

- Cloud Infrastructure/Cloud Servers
  - Azure environment
  - AWS environment
  - Office 365
  - Alegeus/Salesforce/Cobra Point/BSwift (Non-Clarity Controlled)
    - Contact Linda Spitale (Platform VP)
      - lspitale@claritybenefitsolutions.com
  - Clarity Portal
- Premise Infrastructure/Premise Servers
  - Printer /Servers
    - NJ—No Active Servers
    - AZ—No Active Servers

Ancillary Systems/Age/Location

- Infrastructure Clark and Mesa
- Servers
- Printing

- Wireless access points (Clark and Mesa)
- Switches (Clark and Mesa)

Risk Levels and Analysis

Disaster Level Code	
Level I	**Level 1**
Main Building eliminated	Software eliminated
Server Room eliminated	Communication lines eliminated
Level 2	**Level 3**
Cloud Access down	Road hazard (building intact and operational)
Communication lines down	Weather event (snow, flood, hurricane)

Strength	**Weakness**
Multiple locations	Plan testing
Newer technologies	Communications
Virtual Environment	Waste Data
Opportunity	**Threat**
Move to Azure cloud 100%	Vendors
Active-active cluster	Proprietary replacement costs
Multi-location active-active	Internal

Action Plan/Testing

- Installation, recovery documents, and list of customers/contacts are stored in the cloud at:
    i. Google Drive in cloud
    ii. See Team for secure information
- Contacting outside entities method depends on the availability of resources. Should the internet be down, move to ii. Should the building be on lockdown or quarantine then move to iii.
    i. Email
    ii. Work Phone
    iii. Cell Phone
- For premise equipment there needs to be a new location identified to house the systems.
    i. Min 10 miles from corporate will ensure power grid and enough acreage distance from primary.
- The Azure/AWS environment is in a secure CO/LO and will be available
- Salesforce and Portal Data is cloud based and is readily available via Internet to the CO/LO
- Office 365 is in the cloud and will be available
    i. Access Workplace (OS33) from an outside source
        1. HTTPS://beneflex.os33.com
    ii. Email Access
        1. HTTPS:// outlook.office365.com/owa/claritybenefitcolutions.com
- 1st Non-Azure System to come online
    i. Active Directory
- 2nd Non-Azure System to come online
    i. VM Ware servers (SQL)

- 3rd Non-Azure System to come online
    i. Non-Premise based cloud systems

Secondary Plan/Testing (Plan B)

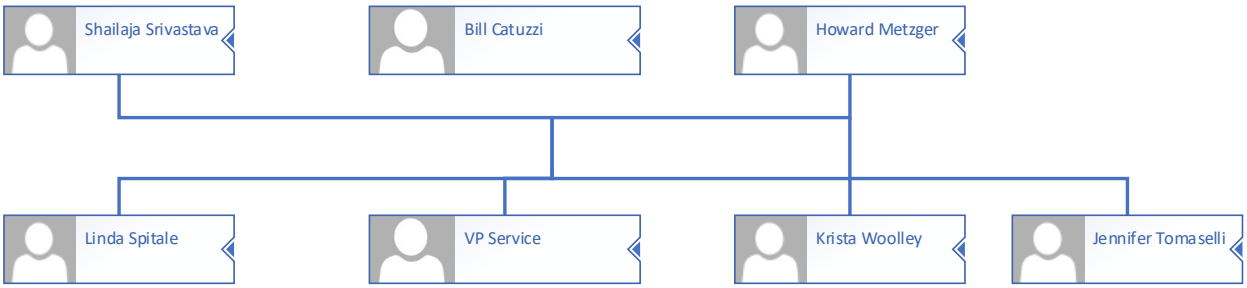
- Vendor Dependent
- Contact vendors on list for cadence and restore sequence

Postmortem process/Lessons Learned

- System recovery
- Time to recover
- Missed systems
- Dollars lost
- Product lost
- Image/Press
- Confidence in IT Department
- Staged for next issue

Communications Tree

Who Can Declare A Disaster
Who Calls Who



- Who can declare a disaster?
  - Bill Catuzzi—Chief Executive Officer
    - bcatuzzi@claritybenefitsolutions.com
  - Howard Metzger—Executive Vice President
    - hmetzger@claritybenefitsolutions.com
  - Shailaja Srivastava — Vice President Information Technology
    - ssrivastava@claritybenefitsolutions.com
- Top Level Communicates to:
  - VP, Service; areas of responsibility:
    - Consumer Benefits and COBRA Benefits for clients, brokers, and partners
    - Participant Call Center
  - Jennifer Tomaselli—VP, Benefit Technology; areas of responsibility:
    - Benefit Administration and Benefit Billing for clients, brokers, and partners
    - Benefit Administration Call Center
    - jtomaselli@claritybenefitsolutions.com
  - Krista Woolley—Chief Marketing Officer; areas of responsibility:
    - Clarity Benefit Solutions Portal
    - Clarity Benefit Solutions Website
    - kwoolley@claritybenefitsolutions.com
  - Linda Spitale—VP, Technology Initiatives; areas of responsibility:
    - Application Vendors
    - lspitale@claritybenefitsolutions.com
  - Division Vice Presidents or approved representatives are charged with notification of respective Partners, Brokers, Clients, Participants, and Vendors. In the event of a disaster contacts will be informed of known circumstances.
    - Client Contact Information for The Group Insurance Trust of the California Society of Certified Public Accountants
      - Contact Name: Mayu Kozuka—CFO
      - Contact Phone: 650-522-3256
      - Contact Email: mayu.kozuka@calcpahealth.com

Clarity Benefit Solutions

Incident Response Policy	Created: 5/7/2018, Updated 08/3102024
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 7

Clarity Benefit Solutions is hereinafter referred to as "the company."

1.0 Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. This policy covers all incidents that may affect the security and integrity of the company's information assets, and outlines steps to take in the event of such an incident.

2.0 Purpose

This policy is intended to ensure that the company is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective.

3.0 Scope

The scope of this policy covers all information assets owned or provided by the company, whether they reside on the corporate network or elsewhere.

4.0 Policy

4.1 Types of Incidents

A security incident, as it relates to the company's information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

- Electronic: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.

- Physical: A physical IT security incident involves the loss or theft of a laptop, mobile device, Smartphone, tablet, portable storage device, or other digital apparatus that may contain company information.

4.2 Preparation

Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.

Additionally, prior to an incident, the company must ensure that the following is clear to IT personnel:

- What actions to take when an incident is suspected.
- Who is responsible for responding to an incident.

The company must have discussions with an IT Security company that offers incident response services before such an incident occurs in order to prepare an emergency service contract. This will ensure that high-end resources are quickly available during an incident.

Finally, the company should review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of customer data), and ensure that its incident response plans adhere to these regulations.

4.3 Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.

4.4 Electronic Incidents

When an electronic incident is suspected, the company's goal is to recover as quickly as possible, limit the damage done, and secure the network. The following steps should be taken in order:

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.

2. Disable the compromised account(s) as appropriate.

3. Report the incident to the IT Manager.

4. Backup all data and logs on the machine, or copy/image the machine to another system.

5. Determine exactly what happened and the scope of the incident. Was it an accident? An attack? A Virus? Was confidential data involved? Was it limited to only the system in question or was it more widespread?

6. Notify company management/executives as appropriate.

7. Contact an IT Security consultant as needed.

8. Determine how the attacker gained access and disable this access.

9. Rebuild the system, including a complete operating system reinstall.

10. Restore any needed data from the last known good backup and put the system back online.

11. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.

12. Reflect on the incident. What can be learned? How did the Incident Response team perform? Was the policy adequate? What could be done differently?

13. Consider a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

4.5 Physical Incidents

Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable policies, such as those covering encryption and confidential data, should be reviewed.

Physical security incidents are most likely the result of a random theft or inadvertent loss by a user, but they must be treated as if they were targeted at the company.

The company must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

4.5.1 Response

Establish the severity of the incident by determining the data stored on the missing device. This can often be done by referring to a recent backup of the device. Two important questions must be answered:

1. Was confidential data involved?
    a. If not, refer to "Loss Contained" below.
    b. If confidential data was involved, refer to "Data Loss Suspected" below.

2. Was strong encryption used?
    a. If strong encryption was used, refer to "Loss Contained" below.
    b. If not, refer to "Data Loss Suspected" below.

4.5.2 Loss Contained

First, change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the IT Manager. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

4.5.3 Data Loss Suspected

First, notify the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

4.6 Notification

If an electronic or physical security incident is suspected to have resulted in the loss of third-party or customer data, follow applicable regulations and/or industry breach disclosure laws and append the regulations to this policy.

4.7 Managing Risk

Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical data and systems from these risks is of paramount importance to the company.

4.7.1 Risk Assessment

As part of the risk management process, the company must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the company's critical or confidential information. The process must include the following steps:

a. Scope the assessment. Determine both the physical and logical boundaries of the assessment.

b. Gather information. Determine what confidential or critical information is maintained by the company. Determine how this information is secured.

c. Identify threats. Determine what man-made and natural events could affect the company's electronic information.

d. Identify Vulnerabilities. After threats have been identified, determine the company's exposure to each threat. External assessments may be useful here, as covered in the Network Security Policy.

e. Assess Security Controls. After vulnerabilities have been cataloged, determine the efficiency of the company's security controls in mitigating that vulnerability.

f. Determine the potential impact of each vulnerability being exploited. Would the event result in loss of confidentiality, loss of integrity, or loss of availability of the information?

g. Determine the company's level of risk. Based on the information gathered in the previous steps, make a determination to the company's level of risk of each event.

h. Recommend security controls. Security controls that will mitigate the identified risks are evaluated during this step. Consider cost, operational impact, and effectiveness of each control.

i. Document the risk assessment results. The final step is to document the risk assessment, including the results of each step.

4.7.2 Risk Management Program

A formal risk management program must be implemented to cover any risks known to the company (which should be identified through a risk assessment), and insure that reasonable security measures are in place to mitigate any identified risks to a level that will ensure the continued security of the company's confidential and critical data.

4.8 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Malware Short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.

Mobile Device A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

Trojan Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbors a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

Virus Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or

via network-connected computers and file systems.

WEP Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WPA Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

7.0 Revision History

Revision 1.0, 5/7/2018

Clarity Benefit Solutions Media, Data Destruction Sanitization Policy

1. Overview

Clarity Benefit Solutions regularly stores sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media reach end of life, sensitive information on surplus equipment and media must be properly destroyed and otherwise made unreadable to protect Personal Health Information (PHI) or Personally Identifiable Information (PII).

2. Purpose

Proper disposal and disposition of surplus computer hardware and other storage media manages risks of security breach and inappropriate information disclosure. Broadly, exposure to the company takes the form of:

- **Violation of Software License Agreements** - Most software is licensed for use on either a single computer system, to a single person, or to an organization. Typically, licenses are not transferable. Even when licenses are transferable, there are generally specific requirements that must be met to affect a transfer. Allowing a third-party access to licensed software without proper transfer of the license may be a breach of the license agreement and may subject the state or the recipient of the software to claims and/or damages.

- **Unauthorized Release of Confidential Information or PII** - Allowing an unauthorized person access to PHI or PII can subject Clarity Benefit Solutions to claims for damages.

This policy is designed to address proper disposal procedures for PHI and/or PII from Clarity Benefit Solutions surplus assets prior to their disposal. Proper sanitization and disposal procedures are key to ensuring data privacy and license compliance.

3. Scope

This policy applies to all Clarity Benefit Solutions staff.

4. Policy

A. GENERAL

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled and managed according to Clarity Benefit Solutions Data Retention guidelines. Data remains present on any type of storage device (whether fixed or removable) even after a disc is “formatted”, power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented.

B. DATA DISPOSAL PROCEDURES

All computer desktops, laptops, hard drives, and portable media must be processed through the Information Technology for proper disposal. Paper and hard copy records shall be disposed of in a secure manner as specified by the archiving and destruction policy. The IT Department shall ensure procedures exist and are followed that:

- Address the evaluation and final disposition of sensitive information, hardware, or electronic media regardless of media format or type.

- Specify a process for making sensitive information unusable and inaccessible. These procedures should specify the use of technology (e.g., software, special hardware, etc.) or physical destruction mechanisms to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed.

- Authorize personnel to dispose of sensitive information or equipment. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed. Approved disposal methods include:

    - **Physical Print Media** shall be disposed of by one (or a combination) of the following methods:

        - *Shredding* - Media shall be shredded using Clarity Benefit Solutions issued and approved cross-cut shredders

        - *Shredding Bins* - Disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor

        - *Incineration* – Materials are physically destroyed using licensed and bonded information disposal contractor

    - **Electronic Media** (physical disks, tape cartridge, CDs, flash drives, printer and copier hard drives, etc.) shall be disposed of by one of the methods:

        - *Overwriting Magnetic Media* - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitization

        - *Degaussing* - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state

        - *Physical Destruction* – implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated

IT documentation, hardware, and storage that have been used to process, store, or transmit PHI or PII shall not be released into general surplus until it has been sanitized and all stored information has been cleared using one of the above methods.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the Clarity Benefit Solutions internal application development and release methodology. Examples of control documentation includes:

- On-demand documented procedures related to surplus disposal of hardware and software

- Data destruction and surplus logs of equipment identified for disposal

- Physical evidence of sanitized assets and/or data destruction/cleansing devices

Clarity Benefit Solutions Media, Data Destruction Sanitization Policy

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all Clarity Benefit Solutions staff handling sensitive hard copy documents or responsible for managing data and hardware assets in the organization.

8. Policy Version History

Version	Date	Description	Approved By
1.0	04/27/2022	Initial Policy Drafted	Ron Angelo

Clarity Benefit Solutions

Clarity Benefit Solutions is hereinafter referred to as "the company."

1.0 Overview

Consistent standards for network access and authentication are critical to the company's information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

2.0 Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3.0 Scope

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the company's externally-reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

4.0 Policy

4.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.

- Users will be granted least amount of network access required to perform his or her job function.

- Users will be granted access only if he or she accepts the Acceptable Use Policy.

- Access to the network will be granted in accordance with the Acceptable Use Policy.

4.2 Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., firstname-lastname, or firstinitial-lastname, etc.)

- Accounts must be password protected (refer to the Password Policy for more detailed information).

- Accounts must be for individuals only. Account sharing and group accounts are not permitted.

- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.

- Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the IT Vice President or executive team, or as required by applicable regulations or third-party agreements.

4.3 Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, that employee's account can be disabled. Human Resources must create a process to notify the IT Vice President in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

4.4 Authentication

User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then authentication should occur on the local machine.

4.5 Use of Passwords

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the company's Password Policy.

4.6 Remote Network Access

Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, the company encourages additional scrutiny of users remotely accessing the network. Due to the elevated risk, company policy dictates that when accessing the network remotely two-factor authentication (such as smart cards, tokens, or biometrics) must be used. Remote access must adhere to the Remote Access Policy.

4.7 Screensaver Passwords

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver passwords are required to be activated after 15 minutes of inactivity.

4.8 Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to corporate standards with regard to antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. This policy will be enforced with product that provides network admission control.

4.9 Encryption

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network,

whether the transmission occurs internal to the company network or across a public network such as the Internet.

4.10 Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Vice President.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

4.11 Non-Business Hours

While some security can be gained by removing account access capabilities during non-business hours, the company does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because the company's business requires all-hours access.

4.12 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Vice President and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Antivirus Software An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats,

including Trojans, spyware, and other malware.

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Biometrics The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Password A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Smart Card A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

Token A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

7.0 Revision History

Revision 1.0, 5/7/2018
Revision 2.0, 12/21/2022

Operations Security Policy

Owner: Vice President, Information Technology

Effective Date: 07/01/2022

Purpose

To ensure the correct and secure operation of information processing systems and facilities.

Scope

All Clarity Benefit Solutions information systems that are business critical and/or process, store, or transmit company data. This Policy applies to all employees of Clarity Benefit Solutions and other third-party entities with access to Clarity Benefit Solutions networks and system resources.

Operations Security

Documented Operating Procedures

Operating procedures shall be documented and made available to all users who need them.

Change Management

Changes to the organization, business processes, information processing facilities, and systems that affect information security in the production environment and financial systems shall be controlled. All significant changes to in-scope systems must be documented.

Change management processes shall include:

- Processes for planning and testing of changes, including remediation measures
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders
- Documentation of all emergency changes and subsequent review
- A process for remediating unsuccessful changes

Capacity Management

The use of processing resources and system storage shall be monitored and adjusted to ensure that system availability and performance meets Clarity Benefit Solutions requirements.

Human resource skills, availability, and capacity shall be reviewed and considered as a component of capacity planning and as part of the annual risk assessment process.

Scaling resources for additional processing or storage capacity, without changes to the system, can be done outside of the standard change management and code deployment process.

Separation of Development, Staging and Production Environments

Development and staging environments shall be strictly segregated from production SaaS environments to reduce the risks of unauthorized access or changes to the operational environment. Confidential production customer data must not be used in development or test environments without the express approval of the Chief Technology Officer or Vice President of Technology Initiatives.

For a full description, see the Data Management Policy for a description of Confidential data. If production customer data is approved for use during development or testing, it shall be scrubbed of any such sensitive information whenever feasible.

Systems and Network Configuration, Hardening, and Review

Systems and networks shall be provisioned and maintained in accordance with the configuration and hardening standards in Appendix A to this policy.

Firewalls shall be used to control network traffic to and from the production environment in accordance with this policy.

Production Firewall Rules shall be reviewed at least annually. Tickets shall be created to obtain approvals for any needed changes.

Protection from Malware

To protect the company's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware protections shall be utilized on all employee issued laptops except for those running operating systems not normally prone to malicious software. Additionally, threat detection and response software shall be utilized for company email. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats.

Clarity Benefit Solutions should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition updates should be configured to be downloaded and installed automatically whenever current updates are available. Known or suspected malware incidents must be reported as a security incident.

It is a violation of company policy to disable or alter the configuration of anti-malware protections without authorization.

Information Backup

The need for backups of systems, databases, information and data shall be considered and appropriate backup processes shall be designed, planned and implemented. Security measures to protect backups shall be designed and applied in accordance with the confidentiality or sensitivity of the data. Backup copies of information, software and system images shall be taken regularly to protect against loss of data. Backups and restore capabilities shall be periodically evaluated, not less than annually.

Clarity Benefit Solutions does not regularly backup user devices like laptops. Users are expected to store critical files and information in company-sanctioned file storage repositories.

Backups are configured to run daily on in-scope systems. The backup schedules are maintained within the backup application software.

Logging & Monitoring

Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or Confidential data.

Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator & Operator Logs

System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

File Integrity Monitoring and Intrusion Detection

Clarity Benefit Solutions production systems shall be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.

Alerts shall be configured for suspicious conditions and engineers shall review logs on a regular basis.

Unauthorized intrusions and access attempts or changes to Clarity Benefit Solutions systems shall be investigated and remediated in accordance with the Incident Response Plan.

Control of Operational Software

The installation of software on production systems shall follow the change management requirements defined in this policy.

Technical Vulnerability Management

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning, penetration tests, and the bug bounty program.

External vulnerability scans shall be run on the production environment at least quarterly. Interior vulnerability scans shall be run against test environments which mirror production configurations.

Penetration tests of the applications and production network shall be performed at least annually. Additional scanning and testing shall be performed following major changes to production systems.

The IT and Engineering departments shall evaluate the severity of vulnerabilities, and if it is determined to be a critical or high-risk vulnerability, a service ticket will be created. The Clarity Benefit Solutions assessed severity level may differ from the level automatically generated by

scanning software or determined by external researchers based on Beneflex, Inc's internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Vulnerabilities assessed by Clarity Benefit Solutions shall be remediated in the following timeframes:

Determined Severity	Remediation Time
Critical	**10 Days**
High	**15 Days**
Medium	**60 Day**
Low	**90 Days**
Informational	**As needed**

Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

Restrictions on Software Installation

Rules governing the installation of software by users shall be established and implemented in accordance with the Clarity Benefit Solutions Information Security Policy.

Information Systems Audit Considerations

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

Exceptions

Requests for an exception to this policy must be submitted to the Chief Technology Officer or Vice President of Technology Initiatives for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Chief Technology Officer or Vice President of Technology Initiatives. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author
1.1	20-July-2022	Initial Approved	Ron Angelo
2.0	04-Jan-2023	Updated with current information	Shailaja Srivastava

Clarity Benefit Solutions

Password Policy	Created: 5/7/2018, Updated 08/3102024
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 4

Clarity Benefit Solutions is hereinafter referred to as "the company."

1.0 Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

2.0 Purpose

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

3.0 Scope

This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

4.0 Policy

4.1 Construction

Passwords can be a weak link in a security infrastructure. Strong passwords are often difficult to remember, which leads to frequent resets and/or users violating policy by writing down their passwords. Because of this, the organization specifies that two factor authentication be used in any situation where passwords are normally used. This may be in the form of a smart card, hardware or software token, biometrics, or another method that greatly enhances security.

The organization recognizes, however, that not every system (internal and external) is compatible with two-factor authentication. Where a password must be used, the organization mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 12 characters

- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)

- Passwords should be comprised of a mix of upper and lower case characters

- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary

- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)

- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well, for example an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.2 Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone

- Users must not share their passwords with others (co-workers, supervisors, family, etc.)

- Users must not write down their passwords and leave them unsecured

- Users must not check the "save password" box when authenticating to applications

- Users must not use the same password for different systems and/or accounts
- Users must not send passwords via email
- Users must not re-use passwords

4.3 Change Frequency

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 180 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.

4.4 Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the IT Manager. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Manager will request that the user, or users, change all his or her passwords.

4.5 Applicability of Other Policies

This document is part of the organization's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Password A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 5/7/2018

Clarity Benefit Solutions

Physical Security Policy	Created: 5/7/2018
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 8

Clarity Benefit Solutions is hereinafter referred to as "the company."

1.0 Overview

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on the company's physical network infrastructure. In order to secure the company data, thought must be given to the security of the company's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

2.0 Purpose

The purpose of this policy is to protect the company's physical information systems by setting standards for secure operations.

3.0 Scope

This policy applies to the physical security of the company's information systems, including, but not limited to, all company-owned or company-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting the company's office is covered by this policy.

Please note that this policy covers the physical security of the company's Information Technology infrastructure, and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlap, care must taken to ensure that this policy is consistent with any existing physical security policies.

4.0 Policy

4.1 Choosing a Site

When possible, thought should be given to selecting a site for IT Operations that is secure and free of unnecessary environmental challenges. This is especially true when selecting a datacenter or a site for centralized IT operations. At a minimum, the company's site should meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters.

- A site should not be located in an area where the crime rate and/or risk of theft is higher than average.

- A site should have the fewest number of entry points possible.

If these criteria cannot be effectively met for any reason, the company should consider outsourcing its data in whole or in part to a third-party datacenter or hosting provider, provided that such a company can cost effectively meet or exceed the company's requirements.

4.2 Security Zones

At a minimum, the company will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure the company's assets. In addition to this the company must provide security in layers by designating different security zones within the building. Security zones should include:

Public This includes areas of the building or office that are intended for public access.

- Access Restrictions: None

- Additional Security Controls: None

- Examples: Lobby, common areas of building

Company This includes areas of the building or office that are used only by employees and other persons for official company business.

- Access Restrictions: Only company personnel and approved/escorted guests

- Additional Security Controls: Additional access controls should be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged if possible.

- Examples: Hallways, private offices, work areas, conference rooms

Private This includes areas that are restricted to use by certain persons within the company, such as executives, scientists, engineers, and IT personnel, for security or safety reasons.

- Access Restrictions: Only specifically approved personnel

- Additional Security Controls: Additional access controls must be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged. Additionally, an alarm system should be considered for these areas that will alert to unauthorized access.

- Examples: Executive offices, lab space, network room, manufacturing area, financial offices, and storage areas.

4.3 Access Controls

Access controls are necessary to restrict entry to the company premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with the company's guidelines for their use.

4.3.1 Keys & Keypads

The use of keys and keypads is acceptable, as long as keys are marked "do not duplicate" and their distribution is limited. These security mechanisms are the most inexpensive and are the most familiar to users. The disadvantage is that the company has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, good security can be obtained with keys and keypads.

4.3.2 Keycards & Biometrics

While keycards and biometrics are allowable forms of access controls, the company does not require their use at this time.

Keycards and biometrics have an advantage over keys in that access policies can be tuned to the individual user. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorized. Perhaps best of all, these methods allow for control over exactly who possesses the credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled. The granular control offered by keycards and biometrics make them appealing access control methods.

4.3.3 Alarm System

A security alarm system is a good way to minimize risk of theft, or reduce loss in the event of a theft. The company mandates the use of professionally monitored alarm

system. The system must be monitored 24x7, with company personnel being notified if an alarm is tripped at any time.

4.4 Physical Data Security

Certain physical precautions must be taken to ensure the integrity of the company's data. At a minimum, the following guidelines must be followed:

- Computer screens should be positioned where information on the screens cannot be seen by outsiders.

- Confidential and sensitive information should not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.

- Users must log off or shut down their workstations when leaving for an extended time period, or at the end of the workday.

- Network cabling should not run through unsecured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).

- The company recommends disabling network ports that are not in use.

4.5 Physical System Security

In addition to protecting the data on the company's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

4.5.1 Minimizing Risk of Loss and Theft

In order to minimize the risk of data loss through loss or theft of company property, the following guidelines must be followed:

- Unused systems: If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.

- Mobile devices: Special precautions must be taken to prevent loss or theft of mobile devices. Refer to the company's Mobile Device Policy for guidance.

- Systems that store confidential data: Special precautions must be taken to prevent loss or theft of these systems. Refer to the company's Confidential Data Policy for guidance.

4.5.2 Minimizing Risk of Damage

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

- Environmental controls should keep the operating environment of company systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.

- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.

- Strong magnets must not be used in proximity to company systems or media.

- Except in the case of a fire suppression system, open liquids must not be located above company systems. Technicians working on or near company systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto company systems.

- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.

4.6 Fire Prevention

It is the company's policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of the company's office. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.

- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.

• Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.

• Only electrical equipment that has been approved by Underwriters Laboratories and bears the UL seal of approval must be used.

• Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if possible.

• Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.

• A smoke alarm monitoring service must be used that will alert a designated company employee if an alarm is tripped during non-business hours.

4.7 Entry Security

It is the company's policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimizing risk to company systems and data. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall security policy.

4.7.1 Use of Identification Badges

Identification (ID) badges are useful to identify authorized persons on the company premises. The company has established the following guidelines for the use of ID badges.

• Employees: ID badges are not required.

• Non-employees/Visitors: Visitor badges are not required, though generic visitor badges are encouraged.

4.7.2 Sign-in Requirements

The company must maintain a sign-in log (or similar device) in the lobby or entry area and visitors must be required to sign in upon arrival. At minimum, the register must include the following information: visitor's name, company name, reason for visit, name

of person visiting, sign-in time, and sign-out time.

4.7.3 Visitor Access

Visitors should be given only the level of access to the company premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered "trusted" by the company. Examples of a trusted visitor may be the company's legal counsel, financial advisor, or a courier that frequents the office, and will be decided on a case-by-case basis.

4.8 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Biometrics The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Datacenter A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

Keycard A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Keypad A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

Mobile Device A portable device that can be used for certain applications and data storage.

Examples are PDAs or Smartphones.

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

Uninterruptible Power Supplies (UPSs) A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.

7.0 Revision History

Revision 1.0, 5/7/2018

Risk Management Policy

Owner: VP Information Technology

Effective Date: July 1, 2022

Purpose

To define the method for assessing and managing Clarity Benefit Solutions information security risks to achieve the company's business and information security goals.

Scope

The risk assessment process may apply to all business processes, information, information systems, networks, devices, and information processing facilities that are owned or used by Clarity Benefit Solutions applicants, employees, contractors, consultants, vendors, partners, and other users affiliated with Clarity Benefit Solutions, or others using or accessing Clarity Benefit Solutions networks and/or information systems.

Policy

Clarity Benefit Solutions will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is to ensure that the company achieves its stated business and security goals and aims.

Risk Management Strategy

Clarity Benefit Solutions has developed processes to name those risks that would hinder the achievement of its strategic and operational goals. Clarity Benefit Solutions will therefore ensure that it has in place the means to name, analyze, control, and monitor the strategic and operational risks it faces using this risk management policy based on best practices.

The VP IT will ensure the risk management strategy and policy reviews are conducted regularly and that:

- The risk management policy is applied to relevant areas at Clarity Benefit Solutions
- The risk management policy and its operational application are annually reviewed
- Non-compliance is reported to proper company officers and authorities

Practical Application of Risk Management

Clarity Benefit Solutions may use a variety of risk reporting formats for the identification of risks, their classification, and evaluation based on factors such as vendors used, method employed, and the scope of the assessment. In general, and where possible, risks shall be assessed and ranked according to their impact and their likelihood of occurrence. A formal IT risk assessment, network penetration tests, and Clarity Benefit Solutions production application penetration test will be performed at least annually.

In addition, an internal audit of the information security management system (ISMS) (i.e., information security controls and management processes) shall be performed at least annually.

Security risks shall be evaluated at various stages of the software design and development lifecycle as needed.

Risk Categories

Some risks are within the control of Clarity Benefit Solutions while others may be only to a lesser degree. Clarity Benefit Solutions will consider the risks within each of the following categories:

- Technical
- Reputational
- Contractual
- Economic/Financial
- Regulatory/Compliance
- Fraud

Each identified risk will be assessed as to its likelihood and impact. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. The likelihood and impact will be considered together to formulate an overall risk ranking.

Risk Criteria

The criteria for deciding risk are the joint likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of customer data, personally identifiable information (PII), or business critical systems.

For all risk inputs such as risk assessments, penetration tests, vulnerability scans, etc., Clarity Benefit Solutions management shall reserve the right to change automated or third-party provided risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability.

Risk Response and Treatment

Risks will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed. Where Clarity Benefit Solutions chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan.

- Mitigate: Clarity Benefit Solutions may take actions or employ strategies to reduce the risk.
- Accept: Clarity Benefit Solutions may decide to accept and monitor the risk at the present time. This may be necessary for risks that arise from external events.
- Transfer: Clarity Benefit Solutions may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Clarity Benefit Solutions, or insurance may be proper for protection against economic loss.
- Eliminate: The risk may be such that Clarity Benefit Solutions could decide to cease the activity or to change it in such a way as to end the risk.

Risk Management Procedure

The procedure for managing risk will meet the following criteria: Clarity

- Benefit Solutions will keep a Risk Register and Treatment Plan.
- Risks shall be ranked by ‘likelihood' and ‘severity/impact' as critical, high, medium, low, or negligible.
- Overall risk shall be decided through a combination of likelihood and impact.
- Risks may be tagged with a value to estimate potential monetary loss where practical, or may be considered compared to a control objective
- Clarity Benefit Solutions will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously.
- Periodic reports will be made to the senior leadership of Clarity Benefit Solutions to ensure risks are

being mitigated appropriately and following business priorities and goals.

Risk Acceptance Levels

Role	Responsibility
CEO	**Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.**
Engineering Manager	**Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with executive direction.**
CTO/VP IT	**Shall be responsible for adherence to this policy.**

Amendment & Termination of this Policy

Clarity Benefit Solutions reserves the right to modify, amend or terminate this policy at any time.

Exceptions

Requests for an exception to this Policy must sent to the Chief Technology Officer for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Chief Technology Officer and Vice President of Human Resources. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author
1.1	01-July-2022	First Version	Ron Angelo
2.0	04-Jan-2023	Updated with current information	Shailaja Srivastava

Appendix A: Risk Assessment Matrix and Description Key

	RISK = LIKELIHOOD * IMPACT	LIKELIHOOD		
		Highly likely: 3	Somewhat likely: 2	Not likely: 1
IMPACT	Very impactful: 3	9	6	3
	Somewhat impactful: 2	6	4	2
	Not impactful: 1	3	2	1

RISK LEVEL	RISK DESCRIPTION
Low (1-2)	**A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.**
Moderate (3-6)	**A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations**
High (7-9)	**A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.**

IMPACT LEVEL	IMPACT DESCRIPTION
Not impactful (1)	A threat event could be expected to have a limited adverse effect, meaning degradation of mission capability yet primary functions can still be performed; minor damage; minor economic loss; or range of effects is limited to some cyber resources but no critical resources.
Somewhat impactful (2)	A threat event could be expected to have a serious adverse effect, meaning significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor economic loss; or range of effects is significant to some cyber resources and some critical resources.
Very impactful (3)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major economic loss; or range of effects is extensive to most cyber resources and most critical resources.

LIKELIHOOD LEVEL	LIKELIHOOD DESCRIPTION
Not likely (1)	Adversary is unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is unlikely to occur; or threat is unlikely to have adverse impacts.
Somewhat likely (2)	Adversary is somewhat unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is somewhat unlikely to occur; or threat is somewhat unlikely to have adverse impacts.
Highly likely (3)	Adversary is highly likely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is highly likely to occur; or threat is highly likely to have adverse impacts.

Secure Development Policy

Owner: Vice President Information Technology

Effective Date: July 1, 2022

Purpose

To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Scope

All Clarity Benefit Solutions applications and information systems that are business critical and/or process, store, or transmit Confidential data. This policy applies to all internal and external engineers and developers of Clarity Benefit Solutions software and infrastructure.

Policy

This policy describes the rules for the acquisition and development of software and systems that shall be applied to developments within the Clarity Benefit Solutions organization.

System Change Control Procedures

Changes to systems within the development lifecycle shall be controlled using formal change control procedures. Change control procedures and requirements are described in the Clarity Benefit Solutions Operations Security Policy.

Significant code changes must be reviewed and approved by Lead Developer, IT Manager or VP IT before being merged into any production branch.

Software Version Control

All Clarity Benefit Solutions software is version controlled and synchronized between contributors (developers). Access to the central repository is restricted based on an employee's role. All code is written, quality checked, and saved in a local repository before being synchronized to the origin repository.

Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

Restrictions on Changes to Software Packages

Modifications to third-party business application packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Secure Development Environment

Clarity Benefit Solutions shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development

Clarity Benefit Solutions shall supervise and monitor the activity of outsourced system development. Outsourced development shall adhere to all Clarity Benefit Solutions standards and policies.

System Security Testing

Testing of security functionality shall be carried out during development. No code shall be deployed to Clarity Benefit Solutions production systems without documented, successful test results.

System Acceptance Testing

Acceptance testing programs and related criteria shall be established for latest information systems, upgrades and new versions.

Prior to deploying code, a Release Checklist MUST be completed which includes a checklist of all Test Plans which show the completion of all associated tests.

Protection of Test Data

Test data shall be selected carefully, protected and controlled. Confidential customer data shall be protected in accordance with all contracts and commitments. Customer data shall not be used for testing purposes. All date used for testing will be scrubbed and sanitized of any personal identifiable information.

Acquisition of Third-Party Systems and Software

The acquisition of third-party systems and software shall be done in accordance with the requirements of the Clarity Benefit Solutions Third-Party Management Policy.

Exceptions

Requests for an exception to this Policy must be submitted to the Chief Technology Officer for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Chief Technology Officer and the Vice President of Technology Initiatives. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author
1.0	**20-July-2022**	**Initial**	**Ron Angelo**
2.0	04-Jan-2023	Updated with current information	Shailaja Srivastava