**Policies & Procedures - Colligere LLC  
Document History**

| **Date:** | **Comments:** |
| --- | --- |
| 03/01/2022 | Document was created. |
| 03/01/2022 | Risk Assessment Policy has been appended |
| 03/01/2022 | Damage Assessment Policy has been appended |
| 03/01/2022 | Incident Response Plan Appended |
| 03/01/2022 | Employee Training and Development Policy Appended |
| 03/01/2022 | Acceptable Use Policy Appended |

[**Definitions:**](#_heading=h.f11leayex9re) **3**

[**Incident Response Policy:**](#_heading=h.rb0ld3hh70jh) **4**

[Purpose**:**](#_heading=h.jac9yt9094ex) **4**

[Scope**:**](#_heading=h.xf6yu3ncy1an) **4**

[**Teams / Roles :**](#_heading=h.gh1wbk8b4kl) **4**

[Information Security Administrators (ISAs)](#_heading=h.f77sp0iotjg0) 4

[Information Security Managers (ISMs)](#_heading=h.48z6ldnw012m) 5

[The Chief Information Security Officer (CIO)](#_heading=h.2hsyx4wfop11) 6

[The Computer Security Incident Response Team (CSIRT)](#_heading=h.chbqrutdrea7) 6

[**Risk Assessment:**](#_heading=h.xthsf2yj4knq) **7**

[Purpose:](#_heading=h.bmbtkre0kmv5) 7

[Scope:](#_heading=h.tj1jlecustq0) 7

[Resource Requirements:](#_heading=h.jc6makemll90) 7

[**Incident Response Plan**](#_heading=h.hgp9pndzkjhp) **9**

[Purpose:](#_heading=h.n9bnx8eor5hy) 9

[Scope:](#_heading=h.6neibhhkpct2) 9

[**Acceptable Use Policy**](#_heading=h.goh97pgfvpra) **10**

[Purpose:](#_heading=h.y7ai0dtnvcl) 10

[Scope:](#_heading=h.y49opjve01r6) 10

[**Audit Controls and Management**](#_heading=h.qrjozuxvxkw7) **11**

#### 

#### 

#### Definitions:

**Computer Incident -** An occurrence that actually or potentially jeopardizes without permission or authority, the confidentiality, integrity, access of information or an information system; or may be an imminent threat of jeopardizing the aforementioned items or any policy in place protecting these items or systems.

**Malware -** Any software designed to cause disruption, corrupt, provide unauthorized access to, or otherwise destroy the integrity of a system, a network of systems, or the information contained therein.

**Data Breach -** Any access to protected data at any level which is unlawful, secretive, or otherwise unauthorized; regardless of whether the data in question is kept on the premises, system, network, or is removed from the premises, system, or network.

**Personal Identifiable Information (PII) -** Information which, when used either alone or in combination with other information about an individual can uniquely identify the individual in question. Examples of this information include but are not limited to a Passport number, Social Security Number (SSN), Date of Birth (DOB), full name, driver’s license number, home address, or work address.

**Vulnerability** - The quality or state of being exposed to the possibility of being attacked or harmed.

**Security Audit** - Testing and assessing the security of an organization’s assets, infrastructure, and systems against a predetermined standard which is either the industry’s best practice or as close as possible to it.

**Critical Business Functions (CBF)** - Business processes that must be restored in the event of a disruption to ensure the ability to protect the organization's assets, meet organizational needs, and meet regulations.

**Recovery Time Objective (RTO)** - The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources.

**Recovery Point Objective (RPO)** - The point in time before a disruption occurs to which business process data can be recovered.

**Maximum Tolerable Downtime (MTD)** - The total amount of time the system owner is willing to accept for a business process outage.

**Employee vs Supervisor -** Includes all officers of administration, officers of instruction, officers of research, and classified staff. The term “supervisors” includes all employees whose job encompasses supervisory duties, including managers and department heads.

**Professional Development and Training -** Learning undertaken by employees to maintain and advance their skills, knowledge and competencies, specifically as they relate and add value to the job and workplace.

#### Incident Response Policy:

##### Purpose:

This document clearly defines IT roles and responsibilities for the investigation and response of computer security incidents such as, but not limited to, data breaches, malware, and social engineering. These policies ensure Colligere LLC is prepared to respond to cybersecurity incidents, to protect data, and prevent disruption of services by providing the necessary controls for incident response.

##### Scope:

The policies included in this document apply to all information systems under the management of Colligere LLC and their affiliates including personnel with authorized access to assets and information resources.

#### Teams / Roles :

###### Information Security Administrators (ISAs)

The Information Security Administrator is typically responsible for installing, administering, and troubleshooting an organization's security solution. They are also the company's first step in monitoring suspicious activity. They also have the following responsibilities:

* Defending systems against unauthorized access, modification, and/or destruction
* Scanning and assessing network for vulnerabilities
* Monitoring network traffic for unusual activity
* Configuring and supporting security tools such as firewalls, anti-virus software, and patch management systems
* Implementing network security policies, application security, access control, and corporate data safeguards
* Training fellow employees in security awareness and procedures
* Developing and updating business continuity and disaster recovery protocols

###### Information Security Managers (ISMs)

The Information Security Managers’ main role is to manage the IT team and its personnel. In addition to the managerial side, other responsibilities will include:

* Provide information security awareness training to organization personnel.
* Creating and managing security strategies
* Oversee information security audits, whether performed by the organization or third-party personnel.
* Manage security team members and all other information security personnel.
* Provide training to information security personnel during onboarding.
* Evaluate department budget and costs associated with technological training.
* Assess current technology architecture for vulnerabilities, weaknesses, and possible upgrades or improvements.
* Implement and oversee technological upgrades, improvements, and major changes to the information security environment.
* Serve as a focal point of contact for the information security team and the customer or organization.
* Manage and configure physical security, disaster recovery, and data backup systems.
* Communicate information security goals and new programs effectively with other department managers within the organization.

###### The Chief Information Security Officer (CIO)

* + The CIO is one of the people in charge. He or she is in the best position to understand the complexities and specifics of the IT infrastructure and services that run the business.
  + This level of understanding allows the CIO to consider all implications, even those stemming from or affecting operations, technology, and events outside the enterprise.
  + Specifically, the CIO’s role in security should extend to three different areas to maintain a strong security posture.
* During incident response, the CIO will direct orders and receive information for subordinates to achieve working operations again that is up to standard to what they need to be.

###### The Computer Security Incident Response Team (CSIRT)

The Computer Security Incident Response Team (CSIRT) is responsible for the early detection and investigation of security events to determine when a major computer incident has occurred,as well as the cause, and amount of damage done to company assets. This is including but not limited to:

* Directing the processes needed to recover, contain, and remediate security incidents and providing authorization for necessary changes to information systems within Colligere LLC.
* Coordinating the response with external parties when the contracts in place require action by the external party.
* Coordinating with law enforcement, government agencies, peer CSIRTs, and relevant Information Sharing and Analysis Centers (ISACs), when necessary, to identify and investigate relevant security incidents. This includes sharing known external threat and incident information with these organizations.
* Communicate with ISA’s and CIO regularly about the current health and state of Information Systems owned and maintained by Colligere LLC. Including but not limited to quarterly meetings.

#### Risk Assessment:

##### Purpose:

##### Scope:

1. **Identify Company Assets**

| **System** | **Priority** | **RTO** |
| --- | --- | --- |
|  |  |  |

#### 

#### Resource Requirements:

To be functional, the minimum requirements needed for the business to operate are:

Internet Access, Access to file shares (or most recent files), Access to email (send/receive), Access to accounting software (even in a limited capacity), Connectivity between the two buildingsas well as User Workstations/Laptops.

| **Business Process** | **Required Resource Component** | **Description** |
| --- | --- | --- |
|  |  |  |

1. **Identify Threats to Assets**

| **Threat** | **Description** | **Asset(s) Effected** |
| --- | --- | --- |
|  |  |  |

1. **What are the Vulnerabilities in our Assets?**

Some of the vulnerabilities in our assets include:

1. **What are the consequences of a vulnerability being exploited?**

In the event of an exploit, consequences can include but is not limited to:

* Loss of assets
* Information Siphoning
* losing complete control of the affected device with data stored on it
* Loss of data
* Compromised device can be used to exploit other devices
* Elevation of privilege, the attacker can gain greater privileges on their account
* Future Denial of service attacks  
    
  **What Controls can be implemented to reduce the likelihood / impact of a threat occurrence.**

| **Threat** | **Description** | **Controls** |
| --- | --- | --- |
|  |  |  |

#### Incident Response Plan

##### Purpose:

##### Scope:

Incident type:

**Hardware Failure**

1. Determine what failed
2. Determine what the cause of the failure was
3. determine what other systems were affected by the failure
4. Determine if hardware effected needs to be repaired or replaced
5. repair/replace hardware effected
6. Document the failure
7. Create/edit policies regarding system auditing to prevent hardware failure in the future

**User Error**

1. Determine what the error was
2. Identify what the root of the error was
3. Determine what systems could be affected
4. Identify the extent of the damage (Was data corrupted, deleted? Was the system compromised?)
5. Restore any data that was affected by the error
6. Fix the error
7. After incident report
8. Create a policy to prevent this situation in the future
9. Provide training so the error is not made in the future

#### Acceptable Use Policy

##### Purpose:

* To define what is considered acceptable use of systems. Including but not limited to what actions users can perform on company-owned systems and infrastructure

##### Scope:

* These policies would be applicable to all employees of Colligere LLC

**Policy:**

It must be ensured through legal or technical means that Colligere LLC proprietary information stored on electronic and computing devices is protected in accordance with the Data Protection Standard

The use of company-owned and operated email and internet-related services are solely for the purpose of conducting business operations. Email is to be used for company business only. Confidential company information must not be shared outside of the company.

Users may only load corporate data that is essential to business functions to mobile device(s). Employees are responsible to promptly report the theft, loss, or unauthorized disclosure of Colligere LLC-owned devices and proprietary information. Devices must be kept up to date with the manufacturer or network-provided patches.

Access to use or share Colligere LLC proprietary information is only permitted to the extent it is authorized and necessary to fulfill your assigned job duties.

Individual departments are responsible for creating guidelines concerning the personal use of IT systems. In the absence of such policies, employees should be guided by departmental policies on personal use.

At this time Colligere LLC does not provide support for employee-owned personal assistant devices, including but not limited to Alexas, Echos, Siri, or any other PDA devices.

Colligere LLC reserves the right to audit networks and systems on a periodic basis to ensure compliance with AUP

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of [Colligere LLC] internal operations. Examples of management controls include:

· Documented information security training plan with evidence of consistent update and version control of the document

· On-demand review of existing training program information and implementation within the organization

· Completion and employee acceptance logs for completed education

· Completion rate statistics

· On-demand evidence of continuing education and reminders are in place