Ex Libris Cloud Services BCP

Version 3.0

Business Continuity Plan Overview

The Ex Libris Group Cloud Services Business Continuity Plan is a comprehensive statement of actions to be taken before, during and after a disaster. This plan is designed to reduce the risk to an acceptable level by ensuring the restoration of critical functions and services within a short time frame, and all essential production within a longer, but permissible, time frame. This plan identifies the critical functions and services for Ex Libris cloud services and the resources required to support them. Guidelines and recommendations are provided for ensuring that needed personnel and resources are available for disaster preparation, assessment and response to permit the timely restoration of services.

Definitions

Business Continuity Plan (BCP) - a document describing a set of arrangements, resources, and sufficient procedures that enable an organization to respond to a disaster and resume its critical operations within pre-defined time frame without incurring unacceptable operational impacts.

Disaster Recovery Plan (DRP) – a technical document describing the processes, policies, and procedures related to implementing precautionary measures and preparing for the recovery, continuation, or resumption of services in the event a catastrophic event occurs.

Disaster – a sudden, unplanned catastrophic event that causes a complete loss or significant disruption in customer's mission critical services. The primary objective of the plan is to minimize the risk of low-level events and minimize the impact of major high-level events.

Business Continuity Plan Objectives

The principal objective of the business continuity plan is to develop, test and document a well-structured and easily understood plan which will help Ex Libris cloud services recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts Ex Libris cloud services and business operations.

The objectives of this document are:

- Develop a Business Continuity Plan structure for managing a disaster that affects the Ex Libris Cloud Services.
- Document critical information and procedures as required for the implementation of the Business Continuity Plan.
- Present a course of action for restoring critical cloud services within a minimum number of days of initiation of the plan.
- Provide guidelines with an escalation plan for a disaster declaration that will result in the execution of this Business Continuity Plan.
- Describe an organizational structure for carrying out the plan and ensure that all employees fully understand their duties in implementing such a plan.
- Ensure an orderly recovery after a disaster occurs, minimizing risk of lost production or services.

Business Continuity Plan

Ex Libris management has approved the following statement:

- The company shall develop a comprehensive Business Continuity Plan.
- A formal risk assessment shall be undertaken to determine the requirements for the Business Continuity Plan.
- The Business Continuity Plan shall cover all essential and critical infrastructure elements, systems and services, in accordance with key business activities.
- The Business Continuity Plan shall be periodically tested to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All cloud services staff shall be made aware of the Business Continuity Plan and their own respective roles and responsibilities.
- The Business Continuity Plan shall be kept up to date to reflect changing circumstances.

Assumptions of the Plan

The Business Continuity Plan has been developed and maintained based on the following assumptions:

- This document plans for the major/worst case disaster. However, if an outage of services occurs to a lesser degree, this plan will address the incident.
- The cause of the disaster is limited to one Ex Libris data center location (Chicago, Amsterdam, Singapore, Frankfort, Australia or AWS).
- Ex Libris Cloud Services utilizes co-location agreements with leading data centers facilities providers (for example, Equinix) and cloud computing services with AWS.

BCP Team Descriptions and Responsibilities

- **BCP Management Team** - Responsible for the overall direction, decision-making, and approvals required to implement the Business Continuity Plan. The team is comprised of the Chief Information Officer and infrastructure engineering senior management who are responsible for leadership within their respective areas.
- **Business Continuity Coordinator (BCC)** – A member of the BCP Management Team with responsibility for the development, coordination, training, testing and implementation of the Business Continuity Plan. The Senior Director, Infrastructure Engineering will typically lead this role.
- **BCP Team Leaders** - Responsible for carrying out the tasks and provisions of the Business Continuity Plan including assigning tasks to staff, obtaining offsite data backups, contacting vendors, monitoring work progress, and reporting the status to the BCP Management Team. The team is comprised of the Infrastructure Engineering team leaders and managers.
- **Emergency Operations Center (EOC)** – A location established by the BCP Management Team for central coordination during the recovery efforts. This location will typically be established at Ex Libris group Headquarters offices.

Disaster Risks and Prevention

As important as having a Business Continuity Plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, and steps that should be taken to minimize Ex Libris risk. There are many forms of catastrophic loss that can occur. This section lists some of the events and situations that are considered when determining what to include in the plan.

Preventive Measures

Potential Disaster	Preventive Measures
Equipment/hardware failure	Redundant infrastructure - This is addressed by Ex Libris in its architecture and design standards at all infrastructure layers including multiple Firewalls, Switches, Storage controllers, Load balancers, manageable PDU's, cabling, Power sources, and standby hardware. Premium grade hardware support contracts with short SLAs for onsite repair or replacement for all Cloud infrastructure hardware – The result is reduced time for replacement of failed servers, drive arrays, and network equipment. Multi Network providers redundant internet connections - This is addressed by Ex Libris in its network architecture and implementation standards in conjunction with services from the ISP to support the requirements.
System and Software Failure (data corruption, programming errors)	Data backups – At all layers, including platform, application, and customer data. 24/7 application and technical support – This is addressed by the 24/7 Hub (NOC). Use of disk protection shared storage technology at the platform and application level
Power outage	Uninterruptable power supply (UPS) and backup generators to power systems in the event of a power failure - data centers feature full UPS power, back-up systems and N+1 (or greater) redundancy. This service is supplied by the facilities provider. Redundant power, cooling – An effective and efficient cooling infrastructure that is robust enough for the most complex high-power density deployments. This is addressed by Ex Libris in its network architecture and implementation standards in conjunction with services from the facilities provider to support the requirements. Surge protection to minimize the effect of power surges on electronic equipment - This is addressed by the facilities provider by implementing both facilities grade protection as well as surge protected power strips at the rack level.
Malicious Activity (security violations, denial-of-service attack, sabotage, act of terrorism)	Physical access security – 24/7 security, biometric authentication, video surveillance, authorized personnel. Infrastructure security - Hardening, change management procedures, Risk Assessment, patch management, password policy, audit and review by the security team. Network security – Segregation, Vulnerability scans, Intrusion Prevention System (IPS), TLS/SSL encrypted communication. Application security - Security Development Lifecycle (SDL), Penetration tests, vulnerability assessment, OWASP Top10, audit and review by the security team. Data security - Data isolation, encryption, segregation, media sanitization (NIST 800-88). Identity & Access Control - SSO, S/LDAP, SAML/Shibboleth, Role-Based Access Control (RBAC). Monitoring & Incident Management - 24x7 monitoring, security breach notification. Human Resources - Security awareness training, confidentiality agreements, adherence to regulations. Compliance & Audit - ISO 27001, SSAE-16, EU Safe Harbor, Data processing agreements, independent audit.
Natural Disasters	Fire prevention — VESDA (Very Early Smoke Detection Apparatus) installed for early warning; analog

Potential Disaster	Preventive Measures
(earthquakes, floods, storms, tornados, hurricanes, natural fires)	addressable fire detectors at 3 levels installed; automatic high pressure hi-fog system alarms, CO2 fire extinguishers, and flame suppression systems are supplied by the facilities provider. 24/7 onsite facilities support – Operation personnel are 24/7 on site and together with security staff fully trained in basic firefighting (handheld extinguishers) with strict procedures in place to deal with emergencies including evacuation. This is addressed by the facilities provider, Smart Hands Services. Flooding - Flooding is reviewed with the FEMA maps (or equivalent) and 100-year flood plains during building area locations and design. This is addressed by the facilities provider, Smart Hands Services. Earthquakes - The building code takes into consideration the geographical regions, the type of soil the foundation sits on and the function of the building (data centers are occupancy group III), then assigns Seismic Design Categories (A thru F) that structural engineers base their calculations on. This is addressed by the facilities provider.
Ex Libris Facilities, Offices and Personnel Crisis	Ex Libris has multiple offices around the world; Business operations are not dependent on one facility or office. Ex Libris employees are cross trained to perform each other's jobs in their respective areas. Ex Libris employees can securely connect remotely to other offices; When necessary, all employees may work remotely indefinitely. The Ex Libris 24x7 Hub (Network Operation Center/Security Operation Center) continues to work 24x7. Facilities have a backup and restore policy and procedures to validate office and business information restorations. Ex Libris has a redundant infrastructure network of internet service provider line connections.
Hub Outage	The Hub monitoring and control systems are located in the data center. In the event of an outage, the Hub analyst will have the ability to continue to access and manage the cloud. Ex Libris employees can connect remotely with a secure connection and have full management capabilities.
Loss of vendor support	Ex Libris uses multiple vendors and has professional support contracts with other consultants.

Redundancy Strategies

The following are the redundancy strategies available on the Private cloud Services environment:

- **Active/Active Load balancing** - Traffic is split evenly between 2 or more servers for critical servers. Upon failure of one of the servers, traffic is shifted automatically and seamlessly to the working server.
- **Active/Active Anti-virus** – Traffic is split between 2 or more anti-virus scan devices for balancing. The traffic is shifted automatically and seamlessly to the working server.
- **Active/Passive Network** – The External Network comes from a primary dedicated line with automatic failover into a secondary dedicated line. The internal network is redundant at all layers.
- **Active/Passive Multiply ISP providers** – Multi ISP connected to the primary site using Managed Internet Route Optimizer with automatic fail over.
- **Active/Passive Firewall** – Network traffic uses primary Firewall with automatic failover to a secondary Firewall.
- **Active/Active Storage** – Data is split between 2 or more storage controllers for balancing and take over in case of fail.

- **Available on-site server capacity** – Also referred to as “Onsite Cold Equipment.” In the event of a catastrophic hardware failure that cannot be resolved in a timely manner, the virtualized instance of the customer’s hosted environment will be mounted from an existing standby server that has been preloaded with the appropriate OS and administrative applications. Where needed, customer data restoration would then be performed from onsite or offsite backups.

Backup Strategies

Ex Libris has a well-developed backup plan consisting of multiple daily snapshots including a full daily backup. The backups are made to a separate set of disks which offers a much more reliable fast retrieve backup media and is stored at the site and in a remote secured location over a private dedicated fast secured line. This guarantees that at any point in time, in case of a disaster, Ex Libris holds copies of the data onsite and in a remote and secured disk backup. On a regular basis, Ex Libris performs a system backup to back up application files, database files, and storage files. On-site backup are kept for 14 days, off-site backup files are retained for 10 weeks. The privacy controls in practice at the company apply as well to all backup files. All backup files are subject to the privacy controls in practice. The restore procedures are tested on an ongoing basis to ensure rapid restoration in case of data loss.

- **On-site backup** – Full backup for OS platform, application, and customer data are performed at least daily (multiple snapshots during the day for critical services/systems) using storage snapshot technology. The backups are kept for 14 days on-site at a separated set of disks. The snapshots are automatically mounted with specific access restriction values seen by the operating system in a special set of directories allowing for an easy and immediate restore at any time by authorized personnel.
- **Off-site backup** – Full backup for OS platform, application, and customer data are performed daily using snap mirror technology over a private dedicated fast secured network connection from the primary data center to an off-site backup location using the same storage technology as the storage at the primary location. Subject to the privacy controls in practice, Ex Libris maintains the off-site backup locations in the same territory (NA, EMEA, and APAC) as the primary locations with a sufficient best practice physical distance. The backups can be retrieved back to the main data center 24/7 by authorized personnel. The backups are kept at the off-site backup managed locations for 10 weeks.

Disaster Detection and Determination

The detection of an event which could result in a disaster affecting Ex Libris Cloud Services is the responsibility of the Ex Libris 24x7 HUB, or whoever first from the Cloud group who discovers or receives information about an emergency situation developing in one of the functional areas of Cloud Services.

Disaster Notification

Whoever detects the disaster must notify the Private Cloud Operations Sr. Director or Infrastracture Engineering senior management. In addition to providing some fault tolerance in the initial response, this role sharing enables effective use of shifts during the disaster recovery process.

The Private Cloud Operations Sr. Director or Infrastructure Engineering senior management will establish the Emergency Operations Center (EOC) and monitor the evolving situation and, if appropriate, will then notify the BCP Management Team. The complete emergency contact list for the Ex Libris cloud services is included in Appendix A.

Normally, the facilities provider’s Network Operation Center (NOC) and/or the local law enforcement receive the initial alarm notice through their monitoring system capabilities. If the emergency does not activate a normal alarm system, these two parties should immediately be notified by the Private Cloud Operations Sr. Director or Infrastructure Engineering senior management.

Determine Personnel Status

Private Cloud Operations Sr. Director or Infrastructure Engineering senior management will determine the status of personnel working at the time of the disaster. On site safety personnel will affect any rescues or first aid necessary to people physically affected by the disaster. The director will produce a list of those individuals currently present who will be available to aid in the recovery process. Caring for the well-being of people is the first priority immediately following a disaster.

Damage Assessment

To determine how the business continuity plan will be implemented following a sever disruption to service, it is essential to assess the nature and extent of the damage incurred.

Once the appropriate facilities provider's contacts have been notified, the BCP Team Leaders will be contacted so that a preliminary determination can be made whether an onsite damage assessment is required or feasible.

Damage assessment is intended to quickly understand the extent of damage to mission critical systems and the facility that houses. Personnel safety remains the first priority.

During the Assessment, the following areas should be addressed:

- Cause of the disaster or disruption
- Potential for additional disruptions or damage
- Area affected
- Status of physical infrastructure (e.g., structural integrity of data center, condition of electric power, telecommunications, and heating/ventilation/environmental conditions)
- Inventory and functional condition of Ex Libris equipment
- Type of damage to equipment or data (e.g., water, fire, physical impact, electrical surge)
- Estimated time to restore normal services

Disaster Determination

The Damage Assessment process will determine the severity of the disaster and estimate the amount of time required to restore the cloud services back to normal operations.
Cloud Services has classified disasters and emergencies into three levels – minor, major and catastrophic.

- **Minor Disaster** - A minor disaster is characterized by an expected downtime of no more than 48 hours. Damage can be to hardware, software, and/or operating environment. Cloud services could be restored to normal operations at the primary site and repairs can be started as soon as possible:
- **Major Disaster** - A major disaster is characterized by an expected downtime of more than 48 hours but less than 7 days. A major disaster will normally have extensive damage to system hardware, software, networks, and/or operating environment. Cloud services could be restored to normal operation with the assistance of certain recovery teams who will be called to direct restoration of normal operations at the primary site.
- **Catastrophic Disaster** - A catastrophic disaster is characterized by expected downtime of greater than 7 days. The facility is destroyed to the extent that an alternate facility must be used. Damage to the system hardware, software, and/or operating environment requires total replacement / renovation of all impacted systems. The implementation of the Disaster Recovery Plan in a remote recovery site is required to restore cloud services to normal operation.

Disaster Recovery Strategy

DR Strategies for Minor & Major Disasters

Data Loss caused by Hardware or Software Failure

This section details the activities needed to restore data loss or corruption due to a minor or major disaster at the hardware and/or software level.

Root Cause Analysis

- A DR Team Engineer will determine the root cause of the data loss.
- In the event that the loss was caused because of hardware failure, the DR Hardware Response Team will be notified. In the event the loss is attributable to software failure or human error, the DR Application Response Team will be notified.

Data Loss caused by hardware failure

- The virtualized instance of the customer's hosted environment will be mounted from existing standby hardware that has been preloaded with the appropriate operating system and administrative applications.
- The system vendor will be contacted with a request for emergency services.
- If required, data restoration will be performed from an onsite or offsite backup
- Hardware repair or replacement will be performed.
- Customer notification would be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

Data Loss caused by data corruption or application issues

- Software will be repaired or reinstalled, as appropriate.
- Data restoration will be performed from an onsite or offsite backup.
- Customer notification will be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

Service Disruption caused by hardware or facility event

This section details the steps to take to resume services after a minor or major event caused at either the hardware or facilities level.

Root Cause Analysis

- A DR Team Engineer will perform a root cause analysis regarding the service interruption.
- If the event was due to hardware failure, either the DR Hardware Response Team or the facilities provider DR Operations Team will be notified (whichever is applicable).
- If the event was caused by software failure or human error, the DR Application Response Team will be notified

Service Disruption caused by Facilities Provider Failure

- Facilities provider-owned resolution activities will be tracked by the Ex Libris engineer through completion.
- Facilities equipment repair or replacement will be performed.
- Customer notification will be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

Service Disruption Due to Ex Libris' Cloud Services Hardware Failure

- The virtualized instance of the customer's hosted environment will be mounted from an existing standby hardware that has been preloaded with the appropriate OS and administrative applications.
- The system vendor will be contacted with a request for emergency service.
- Hardware repair or replacement will be performed.
- As needed, software configurations will be performed on the repaired or replaced hardware.
- Customer notification will be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

DR Strategy for Catastrophic Disaster

This section details the activities to be performed in response to a catastrophic disaster at the facilities level:

- The BCP Team Leaders, in collaboration with the facilities provider, will evaluate the extent of the facilities loss.
- If the primary facility will be out of service greater than 7 days, customer notification will be updated at Ex Libris Status Portal.
- An assessment of the condition of Ex Libris owned equipment will be performed. Equipment that is still usable will be identified and added to available inventory list for use at recovery site.
- Simultaneously, a predetermined alternate facilities provider will be notified and engaged.
- A list of needed equipment/hardware will be created. The procurement process will be initiated to order the needed equipment/hardware.
- A plan and timeline for implementation of the recovery site will be finalized and distributed to the Ex Libris customer stakeholders.
- The implementation plan will be executed.
- The Ex Libris and customer stakeholders will be notified of resumption of service at the alternative hosting facility.

Locate and Salvage Data and Equipment

Initial goals are to protect and preserve the salvageable computer and networking equipment. Any hardware that can be retrieved will be reclaimed by Ex Libris for use in the Recovery Site. In particular, backup storage media will be identified and protected from the elements. Whenever possible, backup storage medial will be removed to a clean, dry environment away from the disaster site. Consideration of sending engineering as required, to the remote location place of the disaster.

Designate Recovery Site

An inspection of the data center and telecommunication closets will be performed by the BCP Team Leaders to determine what equipment is salvageable and the amount of time needed to restore the salvageable equipment back into working order. A decision regarding the use of a designated remote location will be made. This will provide a temporary location where computing and networking capabilities can be restored until the primary site is available. If estimates indicate that recovery at the original site will require more than 7 days, migration to the remote recovery site will be initiated by notifying and engaging with the predetermined alternate facilities provider.

Systems and Data Recovery

Ex Libris will use salvageable equipment if possible. For equipment that cannot be used and must be replaced, the

Procurement Team will contact the appropriate vendors. Data recovery will be performed using backups retrieved from the offsite backup locations. Initial data recovery efforts will focus on restoring the operating system(s) for each system. Next, mission critical system data will be restored. After system data is restored, individual customer data will be restored.

Return to Restored Primary Sites

During the recovery process at the alternate remote site, physical restoration of the primary data center will begin. When the data center is ready for occupancy, the systems running at the alternate remote site will be moved back to the primary data center.

Transferring Services back to primary Data Center

This section defines the steps to be taken in order to transfer services back to the primary hosting site after the use of a designated recovery site. Operational readiness at the original primary site will be verified prior to the execution of this step. Once verified, the following steps will be initiated:

- Migration schedule availability at the facilities supplier
- Migration schedule availability with the customer
- Cloud Services preparation for migration
- Migration execution
- Systems Acceptance Test (SAT) and User Acceptance Test (UAT) completion
- Notice to Operations of Migration

Recovery Time Objectives and Recovery Point Objectives

RTO - Recovery Time Objectives

In case of a need for a complete recovery, Ex Libris will make an effort to recover the customer’s environment as soon as possible and within 24 hours in HEP. Depending on the nature of the disaster, the recovery may take between few hours to several days and is based on the full backup that is made on a daily basis to our cloud environment.

RPO - Recovery Point Objectives

Ex Libris has adopted a rigid backup procedure to safeguard the customers' data. On a regular basis, Ex Libris performs system backups using best practice industry standards and centralized backup systems, including backups of the infrastructure network, operating systems, application files, database files, and storage files. This includes several backup snapshots a day of all the data. All backup files are subject to the privacy controls in use. Ex Libris has the ability to go back up to 24 hours to restore customer data and 4 hours in HEP. This information stored in a secured offsite remote backup facility that hold full daily backup. The restore procedures are tested on an ongoing monthly basis to ensure rapid restoration in case of data loss. In addition, a full copy of the data is maintained at a remote secured site, thus making sure that we always hold a full copy of the data for recovery purposes.

Plan Maintenance and Testing

A Business Continuity Plan is critical and must be maintained to ensure that it does not become obsolete. This section provides information about the maintenance procedures necessary to keep it up to date.

Business Continuity Coordinator (BCC)

The Business Continuity Coordinator has overall responsibility for the design, development, coordination, implementation, administration, training, awareness programs, and maintenance of the Business Continuity Plan. The BCC will follow the best practices established by the ISO 22301 Certification Standard.

In accordance with this compliance, the Business Continuity Coordinator is responsible for:

- Providing BCP project coordination and management.
- Performing risk evaluation and mitigation as required.
- Developing and obtaining approval for the Business Continuity Strategy.
- Developing and implementing the Business Continuity Plan.
- Developing maintaining, coordination, testing and evaluating the BCP.

Business Continuity Plan Maintenance

The BCP will be annually evaluated and updated. All portions of the plan will be reviewed. Additionally, the plan will be tested on a regular basis and any faults will be corrected. The BCP Management Team is responsible for overseeing the individual components and files and ensuring that they meet standards consistent with the rest of the Plan.

Testing the BCP

The Business Continuity Coordinator will conduct periodic tests of the Business Continuity Plan using different methodologies (such as: structured walk-through exercise, tactical exercise, and technical exercise for the BCP Team Leaders) or a combination of these methodologies. A report will be submitted to the BCP Management Team after the completion of the exercise that will detail the success and/or failure of the exercise. A discussion surrounding any improvements to the plan will occur. Any revisions to the document based upon the results of the test and the discussion in management will be integrated into the document.

Appendix A: BCP & DR Team Contacts

The following list contains the relevant information for the DR Project Team leaders:

Name	Role	Mobile	Email
Ex Libris 24x7 hub	Ex Libris 24/7 Support, and communication	+ *-***-***-***	**********
**********	Ex Libris Sr VP & GM	+*-***-***-****	**********
**********	Ex Libris Sr. Director of Private Cloud Operations	+*-***-***-****	**********
**********	VP Infrastructure Engineering	+***-**-***-****	**********

Name	Role	Mobile	Email
**********	Vice President & Chief Information Security Officer	+***-**-***-****	**********
**********	Vice President, Chief Privacy Officer	+***-**-***-****	**********
**********	Senior Director, Privacy	+***-**-***-****	**********
**********	Director, Infrastructure Engineer	+***-**-***-****	**********
**********	Director, Infrastructure Engineering	+***-**-***-****	**********
**********	Director, Database Administration	+***-**-***-****	**********
**********	Cloud infrastructure Engineer	+***-**-***-****	**********
**********	Cloud Production Engineer	+***-**-***-****	**********
Hosted facilities and vendor support list	Hosted facilities and vendor support list	+ *-***-***-***	**********

* Masked to maintain privacy

For additional stakeholders please refer to the Business Continuity Management Policy.

Record of Changes

Type of Information	Document Data
Document Title:	Ex Libris Group Cloud Services Business Continuity Plan (BCP)
Document Owner:	Meni Toubul - Business Continuity Coordinator

Type of Information	Document Data
Approved by:	Robert Cerniglia – Vice President, Systems Engineering and Architecture
Issued:	Apr 18, 2014
Last Test	Aug 14, 2024
Reviewed & Revised	July 20, 2025

Revision Control

Version Number	Nature of Change	Date Approved
1.0	Initial version	Apr 18, 2014
1.1	Updated – Bar V	Apr 22, 2014
1.2	Updated – Eyal A	Apr 23, 2014
1.3	Review and Update- Tomer S	Feb 04, 2015
1.4	Review and Update- Tomer S	Apr 12, 2016
1.5	Review and Update- Tomer S	Jul 12, 2017
1.6	Review and Update- Tomer S	Dec 14, 2017
2.0	Review and Update- Tomer S	Apr 26, 2018
2.1	Review and Update- Tomer S	Jan 17, 2019
2.2	Review and Update- Tomer S	Aug 11, 2019

Version Number	Nature of Change	Date Approved
2.3	Review and Update- Tomer S	Jan 05, 2020
2.4	Review and Update- Tomer S	Mar 25, 2020
2.5	Review and update- Ellen A	May 06, 2020
2.6	Review and update - Tomer S	Jun 17, 2020
2.7	Review and update - Tomer S	Jul 07, 2021
2.7	Review - Tomer S	May 24, 2022
2.8	Review and update - Meni T	Aug 30, 2023
2.9	Review and update	July 10, 2024
3.0	Review and update	July 20, 2025

Document Distribution and Review

The document owner will distribute this document to all approvers when it is first created and as changes or updates are made. This document will be reviewed and updated annually or upon