National Defence Défense nationale

# Defence 365
# SharePoint Online Implementation Project (SPOIP)
# Enterprise Level Agreement (ELA)
# (Basic)

**Date of Issue:** 11 May 2023
**Version:** 1.0
**Inquiries:** Defence 365 Program Director

The CIO and the Information Management Group | DPI et le Groupe de gestion de l'information
*Delivering timely, trusted and secure information* | *Fournir un accès optimum à l'information fiable et sécure*

Canada

## IMPORTANT NOTICE

The information in this document is intended for use by the Government of Canada (GoC) only and is current as of the document release date.

# Revision History

Changes in this document are listed in the table below using the following conventions:

- Minor updates to formally released versions will result in a version number update (e.g., 1.0 to 1.1).
- A major change will result in a new version (e.g., 1.0 to 2.0).

| Date | Version | Amendment | Author |
|---|---|---|---|
| 2023-02-15 | 0.1 | Initial draft | Phil Gagnon |
| 2023-03-07 | 0.2 | Updated draft | Sev Derghazarian |
| 2013-03-09 | 0.3 | Minor changes in wording throughout to address comments following stakeholder review | Donna LeShano-Cote |
| 2023-04-05 | 0.4 | Incorporated risks as per CIO/DTO BN, and added D365 Change Champion role | Hala Azar |
| 2023-05-11 | 1.0 | Document Release | Donna LeShano-Cote |

## Authorization

**D365 Program Representative** **Approver**

DANG, SARAH 288 Digitally signed by DANG, SARAH 288
Date: 2023.05.18 15:07:17 -04'00'

Sarah Dang, D365 Director Date

**Client SharePoint Online Business Sponsor** **Approver**

Name, Role Date

# Table of Contents

# 1 D365 SharePoint Online / PBMM Enterprise Level Agreement

This enterprise level Basic service agreement is intended to confirm the roles and responsibilities of Defence 365 (D365) Program service providers, and the Early Adopter (EA) organization (below) that will use SharePoint Online (SPO) as an information repository, including content (data) with sensitivity up to Protected B:

**Early Adopter organization name:**

## 1.1 Risks

There are several risks involved with agile implementation. By signing this service agreement, L1 organizations are accepting the following project risks:

1. Addition of yet another managed repository could result in increased effort, user frustration, and misuse of the system if the transition is not properly managed;
2. Stream 1 Early Adopters will likely need to retrofit their MS Teams and SPO sites to implement the new Enterprise Information Architecture (EIA), which is expected for all organizations in Stream 3;
3. Limited network bandwidth at certain sites will not be sufficient to meet the increased data traffic demand, which may lead to poor user experience (UX) for some D365 users;
4. No Disaster Recovery and Business Continuity plan for D365;
5. ISS resources not properly allocated to support this effort.

## 1.2 Agreement Terms

Early Adopter Organizations will:

1. Restrict the migration of information from other repositories until a classification system is put in place, allowing an official Retention and Disposition schedule;
2. Accept the risk of significant changes to their solutions and/or established processes, including the impact of migrating content to additional MS Teams SPO sites;
3. Engage the D365 IM pillar to implement the Departmental standard for Retention and Disposition.

**Note:** Engaging the D365 IM pillar is not a precondition for starting the onboarding process, but a required activity to meet the GoC Standard on Systems that Manage Information and Data (SStMID) for data migration.

The D365 Program team will:

1. Provide limited resources for training, support, and communications that will be updated incrementally and iteratively to reflect learnings from Early Adopter organizations;
2. Provide hands-on support for thirty (30) days post-deployment.

# 2 Appendix A: Stream Approach

Defence 365 provides the opportunity for a modern approach to create, use, and store information in an easy-to-use environment with greater end-user flexibility. However, establishing and fully implementing the controls for transitioning to SPO as an information repository on the D365 platform will take time. A multi-stream approach has been developed that will provide the organization with immediate benefit and value, while evolving capabilities as the deployment is scaled.

- **Stream 1 (Early Adopters):** Adoption of SPO (including MS Teams) as an information repository on the D365 platform without IM compliance, supported by a time-limited intake process;
- **Stream 2 (Supported Adopters):** Adoption of SPO (including MS Teams) as an information repository on the D365 platform with partial IM compliance, supported by business consultations and adoption resources;
- **Stream 3 (Enterprise Adopters):** Adoption of SPO (including MS Teams) as an information repository on the D365 platform with full IM compliance, supported by mature business consultation and migration guidance.

Stream 1 consists of the following:

1. Early Adopters will access Microsoft 365 (M365) applications and services on the D365 platform with the capability to:
    a. Use SPO as an information repository without requiring the same information to also be stored in other repositories (e.g., GC Docs);
    b. Accept the risk of initial deployment not meeting all of the requirements associated with information repositories (e.g., Standard on Systems that Manage Information and Data (SStMID));
    c. Accept the risk that significant resources may be required to make changes to their MS Teams and SPO sites, based upon the platform changes and way forward.
2. Early Adopter organizations will commit resources to:
    a. Self-manage their organizations by providing communications, training, and end-user support;
    b. Support D365 platform development, provide feedback to the project team, and solve problems as required to minimize unexpected/unwanted impacts to the business objectives and performance;
    c. Continue to engage the project team to adapt the implementation of MS Teams and SPO sites, including structure, content, and procedures for advancing to Stream 2 and Stream 3.
3. Early Adopters will implement a minimum set of standards and controls for the provisioned MS Teams and SPO sites, as the starting point for meeting the defined standards.

# 3 Appendix B: Roles & Responsibilities of Key Participants

## 3.1 D365 Program

The D365 Program will provide the following:

1. Required MS Teams and SPO sites;
2. Guidelines for the use of Protected B (PB) content stored in SPO sites;
3. Functional oversight and direction for the use of SPO sites and PB content;
4. Initial onboarding support directly with the client Point of Contact (PoC).

## 3.2 Clients

### SharePoint Online Business Sponsor

The Director or Commanding Officer, as the client SharePoint Online Business Sponsor, will:

1. Endorse the current agreement;
2. Support the project, authorize resources for onboarding and support, and perform important employee-facing activities;
3. Appoint the appropriate personnel to the Site Administrator, Information Management Officer (IMO), and D365 Change Champion roles;
4. Ensure there is support for adopting a new IM repository, which can adapt to changes in the service configuration and/or business processes.

### Microsoft Teams & SPO Site Administrators

Administrators of MS Teams and SPO sites will:

1. Act as the first level of support for client employees;
2. Proactively monitor use for adherence to the standards and guidelines, as provided and updated;
3. Manage site permissions in alignment with existing Department of National Defence (DND) and Canadian Armed Forces (CAF) standards, including the requirements for Protected B information (data);

**Note:** Access to PB supported SPO sites requires enhanced reliability clearance, and the need to know (refer to NDSOD Chapter 6, Table 7: Protected B Information Requirements Breakdown):

http://intranet.mil.ca/assets/DefenceTeam/docs/en/health-safety-security/vcds-ndsod-s06.pdf

4. Collaborate with the SPOIP team on potential risks, challenges, opportunities, and successes.

### Information Management Officer (IMO)

An IMO assigned to the organization will:

1. Act as the second level of support for the client organization to:
   a. Assist the organization to use the platform efficiently;
   b. Steer the organization to Service Management Centres (SMC) for IT-related issues.
2. Proactively monitor use for adherence to the standards and guidelines, as provided and updated;
3. Collaborate with other Early Adopter IMOs on potential risks, challenges, opportunities, and successes.

# 4 Appendix C: Terms & Conditions (Details)

## 4.1 Microsoft Teams & SPO Site Provisioning

1. D365 will provide the client with SPO sites for information with Sensitivity up to Protected B;
2. SPO sites will have a minimal configuration applied, and no content provided by the D365 Program;
3. SPO sites will only be provided with the default Microsoft site experience;
4. Specific configuration items and capabilities will be applied incrementally towards a DND/CAF wide solution;
5. Default Sensitivity Labels will be provided to users in Early Adopter organizations:
    a. "Unclassified Internal" for all files in Teams and SPO sites within the entire tenant, including those in other SPO sites;
    b. "Unclassified External" for all email messages sent using Exchange Online.
6. All users must manually apply Sensitivity Labels when using MS Office desktop and web apps for files on the D365 platform, where the default does not apply;
7. MS Teams/SPO site owners must not change the assigned Sensitivity of MS Teams or SPO sites;
8. Specific requirements for Protected B information (data) are identified below:
    a. Microsoft Teams is not authorized for Protected B information (data) processing and storage, including related SPO sites;
    b. All content uploaded to an SPO PB site must be treated as PB content, and for this reason SPO sites are not open by design and should adopt a need-to-know permission model;
    c. All content labelled PB cannot be sent by email from D365, and must be downloaded and sent by encrypted email from the DWAN;
    d. All content stored on SPO PB sites can only be shared with individuals, and not the entire organization;
    e. All content stored on SPO PB sites will be PB protected and only accessible from the DWAN using managed GFE devices, and unmanaged GFE/BYOD devices will not be supported;
    f. PB information must not be stored outside of PB sites on the D365 platform, unless encrypted as part of the existing PB information handling process;
    g. Although users will have the ability to label files as PB in any Teams, SPO or OneDrive space, they must not store PB information in unapproved locations;
    h. All document libraries on SPO PB sites must by default assign a Sensitivity of Protected B Internal;
    i. Sensitivity of documents lower than Protected B Internal will be reduced by document creators.

# 5 Appendix D: Support & Incidents

As outlined in Appendix B: Roles & Responsibilities of Key Participants, the client site Administrator and/or IMO will respond to member related incidents, service requests, and inquiries. If a reported incident cannot be resolved, the Administrator/IMO will immediately contact the Project Support Team.

Additional information and can be found on the SPO pages in the D365 Portal, including the following:

- Sensitivity Labelling in D365;
- Sensitivity Labelling Quick Reference Guide;
- Sensitivity Labels FAQ.

# 6 Appendix E: Conditions & Risks Acceptance

Defence 365 is a continuously evolving platform. The following outlines conditions and risks for participating in Stream 1 as Early Adopters on the D365 SharePoint Online Implementation Project (SPOIP). Acceptance of the following conditions is required to become an Early Adopter.

## 6.1 Information Governance

1. Stream 1 Early Adopter organizations must understand that participation is iterative. Ongoing Microsoft technical changes, D365 configuration changes, and IM operational governance for D365 may require significantly more time to retrofit Early Adopter sites, including the relabelling of documents, moving content, and adapting to new and changing configurations and standards;
2. Clients participating in Stream 2 and Stream 3 will need to engage in business consultations with the IM pillar for D365 to align with the enterprise information architecture (EIA), and the scope of business functions to be performed by the client organizations.

## 6.2 Adoption & Change Management

An integral part of user adoption is ensuring that appropriate training and communications are prepared for onboarding new D365 users. Currently, the D365 Portal has a dedicated SPO space that includes information and basic training. However, Stream 1 Early Adopter organizations will not receive the entire onboarding “package.” Users in Early Adopter organizations will be asked for their feedback and recommendations, and will be key contributors for finalizing the end state of training and information resources.

## 6.3 Service Management

1. Concept of support and resources for managing D365 as an enterprise-wide platform are currently being defined due to support services that are not yet fully developed, with only limited support resources available for Stream 1 Early Adopters. Early Adopter organizations must accept that only limited support resources will be available, and must work with the D365 Program team to resolve challenges and optimize the solution;
2. Migration activities and support are out of scope for the SPOIP during Stream 1 (Early Adopter) onboarding;
3. Disaster recovery and business continuity plan does not yet exist for D365.

## 6.4 Technical Readiness

1. Department of National Defence (DND) and Canadian Armed Forces (CAF) network bandwidth can vary greatly between different locations due to the main DND access point (1), building-specific bandwidth (2), and building-specific network hardware (3). This may result in poor user experience (UX), and in some locations may also lead to no access to the D365 platform;
2. DND employees and CAF members are currently provided with two accounts, mailboxes, and calendars (i.e., @forces and @ecn.forces). Despite the initiative in progress for migrating users to a single mailbox and calendar, Stream 1 Early Adopters will still have two mailboxes and calendars.