THOMPSON RIVERS UNIVERSITY

Privacy Impact Assessment
Customer Relationship Management (CRM) System
(Microsoft Dynamics 365 & Greymatter)

File: #P19-08 **Date:**

Project Sponsor or Manager	Name: Maggie Fung Department: IT Services	Email: mfung@tru.ca	Phone: 250-828-5326
PIA Drafter/Project Lead:	Name: Andrea Rhodes Department: IT Services	Email: arhodes@tru.ca	Phone: 250-852-7188
Reviewed By	Laurel Wale, Privacy and Access Officer Scott Blackford, Legal Counsel	Email: lwale@tru.ca Email: sblackford@tru.ca	Phone: 250-828-5012 Phone: 250-852-6811

Executive Summary

This Privacy Impact Assessment (PIA) is being conducted using the template developed and adopted by the Government of B.C. This document is a full PIA and is prepared as a result of a previous preliminary PIA that was completed, using an assessment tool that was developed and is used by the University of British Columbia (UBC).

Thompson Rivers University (TRU) is seeking an institution wide Customer Relationship Management (CRM) platform that will streamline functions by supporting processes that are easy for staff to understand and provide the following applications (which are described in detail below): prospect management tools, communication tools, tracking, scheduling, reporting and analysis.

The adoption of this new CRM by TRU will entail sharing significant amounts of data, including personal information and sensitive information from TRU servers at our Kamloops Campus (and backed up at two locations in B.C.), into what is commonly referred to as "the Cloud" (in this case Microsoft's Azure Service located in Canada). The data on TRU servers (and on its backups) will continue to reside at their current location in the TRU data centre on the Kamloops Campus.

This PIA has been prepared by Information Technology (IT) Services Staff and reviewed by TRU's Privacy and Access Office and by TRU Legal Counsel.

The Risk Mitigation Table with recommendations is attached in Appendix A.

Preliminary PIA:

s.13

Definitions

Application (app) - software designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user.

Banner - TRU's Enterprise Resource Planning (ERP) and Student Information System (SIS).

the Cloud – a geographically dispersed network of servers that operates as a single system. There is more than one "Cloud" system.

Constituents – individuals grouped by their relationship to TRU. For the purposes of this PIA, the constituents are: registered students and applicants, prospective students, high school counsellors, employees, homestay families, recruitment agents and agencies, donors, and alumni.

Customer Relationship Management (CRM) System - technology used to develop, sustain, and manage customer data and interactions throughout the customer lifecycle.

Data Bridge – software that integrates any system of records and allows users to extract data from a source, then re-format, process and store that data in various forms.

Data Bridge Agent (or Integration Agent) – in relation to TRU's CRM implementation, this refers to software (in this case, called Greymatter) that sits on a virtual machine and integrates D365 with any system of records with easy to use tools; the data bridge agent manages the copying

and revision of data from TRU databases to the CRM based on data changes in those databases.

Data Controller – the individual or entity that determines the purposes for which and the means by which personal information is processed (collected, used, disclosed, retained, and stored). For the CRM this is TRU.

Data Processor – an individual or organization that processes data on behalf of a data controller. For the CRM this is Microsoft.

Enterprise Service Bus –an integrated platform that provides interaction and communication services for complex software applications such as the CRM.

External Users – users of the CRM who are not employees of TRU (ie: TRU agents, prospects, and students)

Information Security Program – a system for designing and implementing security practices to protect critical business processes and IT assets, and helps organizations develop a holistic approach to securing their technology infrastructure.

IaaS (Infrastructure as a Service) - a service model that delivers computer infrastructure on an outsourced basis to support enterprise operations. Typically, hardware, storage, servers and data center space or network components; it may also include software.

Interactive Service Hub – A dashboard-based interface that shows customer service teams all of the vital information they need for their day in a single place.

Job Scheduler - The scheduler is software that tells the Data Bridge Agent when to trigger a designated process.

Knowledge Base – A repository of information that is used by a customer service team but is visible to everyone. It consists of documents that are categories by subjects.

Platform - A group of technologies that are used as a base upon which other applications, processes or technologies are developed.

PaaS (Platform as a Service) - a cloud computing model that provides customers a complete platform—hardware, software, and infrastructure—for developing, running, and managing applications. The Platform is provided entirely from remote servers rather than on-premises.

SaaS (Software as a Service) - is a software licensing and delivery model in which software is licensed on a subscription basis and is hosted by the licensor remotely from the user.

Solution – A solution is a product, a combination of products, services, or a mix of products and services that a vendor, service provider or value added reseller will offer to their client.

Subprocessing – data processed by a third party on behalf of the data processor.

TRU Tenant – location in the Microsoft Azure Cloud where TRU data is stored.

Part 1 – General

1. Description of the Initiative

TRU is seeking an institution-wide Customer Relationship Management (CRM) solution that will streamline TRU's customer relationship activities by supporting processes that are easy for staff to understand and which provides:

- prospect management tools, used in connection with the identification of prospective students and donors and which provide TRU users with access to: demographic, personal information for prospective students and donors as well as corporate information for prospective donors that are corporations;
- communication tools, which will allow TRU users and external users to send and receive emails, to send and receive text messages and to make and receive phone calls where the external users have explicitly consented to each communication channel;
- tracking capabilities, which will allow TRU users to keep track of information pertaining to: events, preferences of students and donors, communication and interactions with TRU users, programs of interest and semester of interest for students, changes of job positions of donors. Also, tracking of cases associated with prospects, students, agents, donors and other corporate organizations opened by either the external constituent (prospect, students, agents, donors and other corporate organization), or opened by TRU staff on behalf of the external constituent.
- scheduling of appointments with students, prospects, corporate partners and donors, and scheduling of events; and
- reporting and analysis on the effectiveness of services, performance of TRU's conversion and soliciting efforts for external constituents, experience of students across their journey.

The CRM includes two separate, but dependent and integrated components: Greymatter and Microsoft Dynamics 365 (D365). D365 is the Microsoft platform that forms the basis of the CRM. D365 is then modified and supplemented by Greymatter. D365 is the platform that will be primarily responsible for the security and processing of TRU's data in the CRM. These two products will always be used together and function as a single CRM product.

A. Microsoft Dynamics 365 Services (D365)

D365 is a platform that can be used with any system of records; this is housed in a Microsoft Canadian data centre and backed up in another Microsoft data centre located in Canada. These data centres are part of the Microsoft Azure cloud computing services.

Frequency Foundry has advised TRU's IT Services department that Microsoft does not currently use any third party subprocessors in connection with providing D365, and that all processing of data that Microsoft does is carried out solely in Canada. Microsoft's Online Service Terms (OST) state that Microsoft personnel will only process customer data upon instructions from the customer (i.e.: any other processing will be done by machine access only, rather than personnel and no individual will have access to the

data kept by TRU in the Azure Cloud). This also applies to Microsoft's subprocessors that Microsoft may use in the future, for whose compliance Microsoft is responsible.

Frequency Foundry has advised that Microsoft processes metadata arising from D365 in the US, but this is done only to assess performance of D365 and is done via machine access (ie: not by any individual employed by or contracted to Microsoft).

Dynamics 365 is a platform on which applications can be built. There are some prepackaged applications that are offered on Dynamics 365. Greymatter is the application (referred to as a "solution" in the Microsoft Dynamics 365 parlance) that serves the higher education sector with specific tools for Dynamics 365.

Microsoft Azure services provide the Enterprise Service Bus. The Job Scheduler will reside on-site at TRU. It is critical to note that these Azure services contain no sensitive data or personal information, and only act as the scheduler to trigger the Data Bridge Agent to perform the required copying of data to the CRM.

Data used by the CRM will be stored in and accessed from one of Microsoft's Canadian-based data centres. These data centres are part of the Microsoft Azure cloud computing services.

For the CRM project, TRU will be using the following D365 core services across all TRU constituent groups (see Appendix C, Dynamics 365 Licensing Guide, for additional details regarding the access that each license provides):

a. Dynamics 365 **Customer Engagement Plan**
    - This license allows TRU users to use the following, which must also be licensed individually: Dynamics 365 for Sales (Enterprise and Professional), Dynamics 365 for Customer Service (Enterprise and Professional), Dynamics 365 for Field Service, and Dynamics 365 for Project Service Automation. These services allow CRM users to:
        - Modify accounts, contacts, activities, tasks and notes
        - Record time and expense for Dynamics 365 for Project Service Automation
        - Set up and manage the knowledgebase and Interactive Service Hub
        - Update personal information
        - Use reporting and dashboards
        - Edit custom entities (a meaningful collection of data beyond what's provided out of the box)
        - Participate as an end-consumer of Dynamics 365 services such as responding to surveys, or applying for projects
b. Dynamics 365 for **Sales Enterprise**
    - This license allows TRU users full access to complex sales functionality, beyond what is base-line provided by D365. This includes contact management, lead and opportunity management, and prospective donor management;
c. Dynamics 365 for **Sales Professional**
    - This license is similar to Dynamics 365 for Sales Enterprise but with more features and limited access for employee groups who do not require full sales access;

d. Dynamics 365 for **Customer Service Enterprise**
   - This license is required to use the services in Dynamics 365 for Enterprise/Full users. Beyond baseline D365 functionality, it provides a branded, personalized, self-service experience that leverages an organized, searchable knowledge base (in this case, the data in the CRM) to deliver consistent, up-to-date answers;

e. Dynamics 365 for **Customer Service Professional**
   - This license is required to use the services in Dynamics 365 for App/Professional users but is limited in functionality compared to Customer Services Enterprise by the number of features required and the level of scenario complexity;

f. Dynamics 365 for **Case Management**
   - This license allows TRU users to use the functionality desired in tracking, interaction management and communication. It provides incident based tracking for issues that may arise from customers, whether they are external or internal.

g. Dynamics 365 for **Field Services**
   - This license is required to schedule appointments with external constituents and allows for planning for deploying TRU users to specific high school events

h. Dynamics 365 for **Project Service Automation**
   - This license allows TRU users to potentially use Dynamics 365 as a Project Management tool for internal IT and non-IT Projects;

B. Greymatter

Frequency Foundry is a Canadian company based in Calgary, Alberta and is a Microsoft Gold Cloud CRM Partner with a focus on higher education. Frequency Foundry's Greymatter for Dynamics 365 (D365) is a CRM solution built on the Microsoft Dynamics 365 Customer Engagement platform. Greymatter can help manage the full student lifecycle, as well as customer relations with donors and prospective donors and students.

Greymatter is a cloud-based software as a service (SaaS) offering. Greymatter measures, manages and streamlines interactions with constituents across the full student life cycle from first contact as a prospect through to application, admission and alumni. Using the Microsoft cloud, Greymatter includes a comprehensive donor management platform, a student portal, international recruiting agent relationship management, e-commerce functionality, and offers integration to Banner.

Greymatter includes a Data Bridge Agent that integrates D365 with any system of record with easy to use integration tools. Its primary task is to ensure that TRU constituents' data is copied from the following TRU databases to the CRM: Banner, Banner Document Management (BDM), Microsoft Exchange, SharePoint, and TRU's International Student Portal (ISP).

At TRU, Greymatter will integrate and replicate data currently located in and compiled from the selected TRU databases. The Greymatter D365 dashboard will show information customized for individual users "at a glance". Greymatter also provides a set of business processes, forms, views, dashboards, and reports that are pre-created as templates that sit on D365.

TRU will use a virtual machine within the TRU environment to host the Greymatter Data Bridge Agent. This agent manages the copying of data from Banner and other TRU databases to the CRM based on data changes in those databases. The Data Bridge Agent is fully hosted inside of TRU's on-campus infrastructure and no data is shared with Frequency Foundry via the Data Bridge Agent.

Different licenses will be provided to different user groups, based on their departmental needs in regard to the CRM. In addition, while the CRM will take advantage of the listed core services, not all users will receive all access - people who require less access will have less access.

Table 1 - Planned license usage:

Role	Quantity	Usage	Microsoft D365 License Type
IT & Administrators	20	Full Administrative	Customer Engagement
Advancement/Alumni	30	App/Module only	Sales Enterprise
Exams/Delivery Support	15	App/Module only	Cust Svc Enterprise
Marcom	20	App/Module only	Sales Enterprise
PLAR (Prior Learning Assessment and Recognition)	4	Basic/Light License	Team Member
Registrar's Office - Administration	8	Full Administrative	Customer Engagement
Registrar's Office - Admissions	20	Full Administrative	Customer Engagement
Registrar's Office - Advising	18	App/Module only	Cust Svc Enterprise
Registrar's Office - Enrolment Services	24	App/Module only	Sales Enterprise
Registrar's Office - Records	8	App/Module only	Sales Enterprise
Registrar's Office - Recruiting	12	App/Module only	Sales Enterprise
Strategic Partnerships	5	App/Module only	Sales Enterprise
Student Development Staff	75	Basic/Light License	Team Member
TRU General	8	Full Administrative	Customer Engagement
TRU World Admissions	12	Full Administrative	Customer Engagement
TRU World Advisors	11	Full Administrative	Customer Engagement
TRU World Clerks	6	App/Module only	Cust Svc Enterprise
TRU World Marketing	9	App/Module only	Sales Enterprise
TOTAL USERS	**305**		

Table 2 - Proposed uses of the CRM:

Departmental Staff	Proposed CRM Use	Constituent PI affected	Data integration from Banner (and other systems?)	Direct entry into the CRM	May replace existing stand-alone system(s)
Marketing & Communications	• Support marketing campaigns via mass email, newsletters, and analytics	• Students • High school counsellors • Internal constituents	√	√	Yes Campaign management software

	• Social media management • Form creation • Surveys				
Student Development	• Case management for judicial affairs, academic appeals, wellness centre booking system and possible notes. • disability services and counselling • Support for student engagement and alerts.	• Students	√	√	Yes Clockwork System Writing Centre Online Simplicity CRM
Career Ed	• Career management	• Students	√	√	Yes Simplicity Career
Information Technology Services	• Administration of CRM	• All			
Enrolment Services	• Student registration and official student records management. • Advising notes	• Students	√	√	Yes myTRU student portal
Future Students Office	• Student recruitment	• Prospective students Existing students • High school counsellors	√	√	Yes Chat system
Open Learning	• Prior learning assessment & recognition (PLAR) management. • Form replacement	• Prospective students • Existing students	√	√	
TRU World	• Management of International students and agents, study abroad and exchange students	• International. students, • International. agents, • Homestay hosts, • Domestic students, going	√	√	Yes Calendar/booking ISP

	(incoming and outgoing) and homestays placements.	on study abroad/exchange			Simplicity Horizon
Advancement	• Donor management and alumni interactions	• Donors • Alumni • Donor Prospects	√	√	
Athletics	• Event management	• Students • Staff • General public	√	√	

Many of the proposed uses of the CRM will include copying personal information about individuals, including in many cases sensitive and detailed information, to the Microsoft Azure cloud.

2. Scope of this PIA

The scope of this PIA is to assess personal information being collected, used and disclosed to Frequency Foundry and Microsoft through use of the CRM.

3. Related Privacy Impact Assessments

A Preliminary Privacy Impact Assessment (PPIA) has been completed for the CRM project and is attached as Appendix B.

4. Elements of Information or Data

Personal information will be collected, stored and processed in the CRM via a connection with TRU existing software, Banner, and other chosen databases, as well as manual direct input into the CRM by TRU staff or by individuals themselves.

Identified Data Elements that may be included in the CRM listed by Constituent group are listed in the table below. Business contact information is not considered personal information under the BC *Freedom of Information and Protection of Privacy Act* (FIPPA).

In addition to the Identified Data Elements listed, metadata, which may also contain one or more of these data elements, is created by the CRM and machine accessed by Microsoft.

Table 3 – Identified Data Elements by Constituent Group.

Registered Students & Applicants	**Prospective Students**
• Name • Birthdate • Contact information (including address, phone number & email) • Course history including marks • TRU Transcripts • Program information • Advising notes • Counselling notes	• Name • Previous schooling information • Contact information (including address, phone & email) • Academic intentions • Personal profile, which includes information such as Birthdate, communication preferences, allergy or meal preferences (if they are attending events), connections (relationships to

• Transfer Credit / Transcripts from other organizations
• Payment information (financial)
• Records of student interactions with service departments
• Application details
• Date of graduation
• Athletic designations
• Club membership
• Event registration and attendance (provided they check in and acknowledge being there)_
• Correspondence history
• International Student specific information
  ○ Visa
  ○ Study permit information
  ○ Homestay location
  ○ Travel details
  ○ Pictures
  ○ Agent relationships
	other TRU students, users, or other external constituents that TRU may be communicating with eg. 2 prospective students may be siblings, or a prospective student may be child of a donor)
	• Historic Interaction between TRU and the prospective student.
	• Correspondence
	
	High school counsellors
	• Name
	• Contact information
	• School affiliation
	• Student to counsellor relationship
	
	Employees
	• Name
	• Contact information (including phone number & email)
	• Title / Department
	• Employee calendar (either Exchange or Office 365; undecided at this time)
	• Appointment information (either Exchange or Office 365; undecided at this time)
	• Employee notes, which include notes that employees have made for themselves as they use the system. This includes information TRU employees may want to retain on employees of external companies (e.g. Information for TRU employees to share amongst each other who may be collaborating with an external constituent who is an employee)
	• CRM usage history based on audit logs which will provide information on when employees may be accessing the portal and how they are using the portal
	• Personal files are not included.

Homestay families
• Name of primary contact
• Names of additional family members
• Contact information
• Address
• Placement history
• Biographical information (e.g., interests, languages, pets, restrictions, preferences)
• Availability
• Correspondence
	Recruitment agents and agencies
	• Agency name
	  ○ Contact information
	  ○ Location
	  ○ Sub agencies (regional offices)
	▪ Locations
	  ○ Agent (employee) information
	• Agent name
	  ○ Contact information
	• Agent to agency relationships and history

	• Correspondence
Alumni • Name • Birthdate • Athletic and club history when at TRU • Contact information (including address, phone number & email) • Employment information • Historic interactions • Event attendance • Family /friend relationships	**Donors** • Name • Contact information (including address, phone number & email) • Employment information • Historic interactions • Event attendance • Personal profile, which includes information that Advancement staff collect in relation to prospective and existing donors. May also include information such as: Birthdate, communication preferences, allergy or meal preferences (if they are attending events) • Correspondence • Family /friend relationships - (relationships to other TRU students, users, or other external constituents that TRU may be communicating with eg. a prospective student may be child of a donor) • Community involvement • Financial details • Donation history • Giving commitments • Clothing information such as sizes for t-shirts and swag that may be submitted when donors register for events

Part 2 – Protection of Personal Information

Microsoft Privacy Statements: Microsoft has a Privacy Statement that includes multiple webpages that outline its current position on the protection of privacy with regard to data shared

with it via D365. This Privacy Statement is controlled by Microsoft and may be changed unilaterally by Microsoft from time to time without notice.

TRU's proposed contract with Frequency Foundry contains a provision prohibiting Frequency Foundry from intentionally accessing TRU's data or intentionally disclosing TRU's data to a third party, except

i. Where TRU makes such data publicly available;
ii. Where necessary to provide the services contemplated in the agreement; or
iii. As authorized by TRU in writing.

5. Storage or Access outside Canada

(a) Azure. In March 2018, BCNet completed a Privacy Impact Assessment on Microsoft Azure. In this PIA it was found that:

> "Azure has two regions in Canada with data centres in Canada Central (Toronto) and Canada East (Quebec City). The Microsoft Canada Data Centres replicate data within individual datacenters and between the Toronto and Quebec City facilities to ensure that customer data remains available. Redundant, 'in Canada' fibre paths are intended to enable data residency in Canada while also ensuring continuous service delivery." It was noted that "organization data and system metadata used to maintain the service **may reside outside of Canada**".

According to the Microsoft Online Services Terms (March 2019) that form part of the agreement for the CRM all data "at rest" will be stored within TRU's Microsoft Canada data centres (one of Microsoft's Azure cloud computing services). TRU data will be held in the TRU tenant (TRU's space in the Canadian Microsoft data centre). This agreement is silent about whether data in transit stays only in Canada, and based on this, it is necessary to assume that data in transit will not stay in Canada.

(b) Processing: Microsoft's Online Service Terms states that Microsoft's personnel may only process customer data on instructions from the customer; this also applies to any subprocessors Microsoft may employ, for whose compliance with the Online Service Terms Microsoft is responsible. Other processing of data (including processing of metadata) is done by machine access only; such processing is permissible under section 33.1(1)(p.1) of FIPPA. Microsoft is entitled to revise its Online Service Terms from time to time as it sees fit.

(c) Subprocessing: subprocessing services are other processors used by Microsoft to process data when Microsoft hires third parties to provide certain limited or ancillary services on its behalf. The most current list of Microsoft Subprocessors does not indicate any for D365 (Appendix I). However, Microsoft's Online Service Terms provides that Microsoft may hire subprocessors at any time, with notice to users of Microsoft products.

(d) Access Other than by Microsoft: TRU agents, prospects, and students would be able to use the CRM to access only their own personal information or information they have provided to the system about themselves.

(e) U.S. *Clarifying Lawful Overseas Use of Data ("Cloud") Act:* The Cloud Act, brought into force on March 23, 2018, applies to "electronic communications providers" within the subpoena powers of US courts (Microsoft, as a US based company and a provider of cloud

services, is an electronic communications provider under the Act). Microsoft may be required to disclose to US authorities TRU's data in the CRM, including sensitive personal information of TRU students, employees or donors, if such information is subject to a subpoena, court order, warrant, or in the case of an FBI counterintelligence or counterterrorism investigations, a letter request from the FBI. There is therefore a material risk that Microsoft may be required to disclose sensitive TRU data to the US government under the Act.

TRU Legal has looked carefully, including obtaining external legal advice, at the issue of whether making data subject to the *Cloud Act* by using Microsoft (a US company) as a service provider could mean TRU is failing to ensure that data is stored and accessed only in Canada per section 30.1 of FIPPA. Our conclusion is that there is some risk that this may be deemed a breach of s. 30.1, but this risk is low. This conclusion is based on the following:

1. The BC Privacy Commissioner's office has never stated that use of a US service provider would be contrary to s. 30.1 due to the existence of the *Cloud Act*;
2. S. 30.2 expressly contemplates foreign demands for disclosure, and requires that such demands be reported to the minister responsible for FIPPA; and
3. The addition of s.33.1(1)(p.2) is expressly to authorize use of Cloud services that will temporarily process data outside of Canada.

Microsoft Online Service Terms (OST)

The OST states that Microsoft will comply with all laws and regulations applicable to its provision of Online Services, but that it is not responsible for compliance with any laws or regulations applicable to the customer or the customer's industry (such as FIPPA). The customer owns its data that is stored on Microsoft cloud services at all times. The customer also retains the ability to access its customer data at all times, and Microsoft will deal with customer data in accordance with the terms and conditions of the Enrollment (terms of the program license) [NTD: what is "Enrollment"?] and the OST. Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer may extract the data. No more than 180 days after expiration or termination of the customer's use of an Online Service, Microsoft will disable the account and delete customer data from the account.

Microsoft makes specific commitments with respect to safeguarding its customer's data in the OST. According to the OST, Microsoft commits that:

> *Your data will only be used to provide the online services to you and your data will not be used for any other purposes, including for advertising or similar commercial purposes (OST, page 8).*
>
> *Microsoft will not disclose your data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for your data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from you. If compelled to disclose Customer Data or Personal Data to law*

enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so (OST, page 8).

Microsoft has implemented and will maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect your data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. (OST, page 9, 35) Technical support personnel are only permitted to have access to customer information when needed (OST, page 12).

Microsoft further agrees to notify you if it becomes aware of any security incident, and to take reasonable steps to mitigate the effects and minimize the damage resulting from the security incident (OST, page 6).

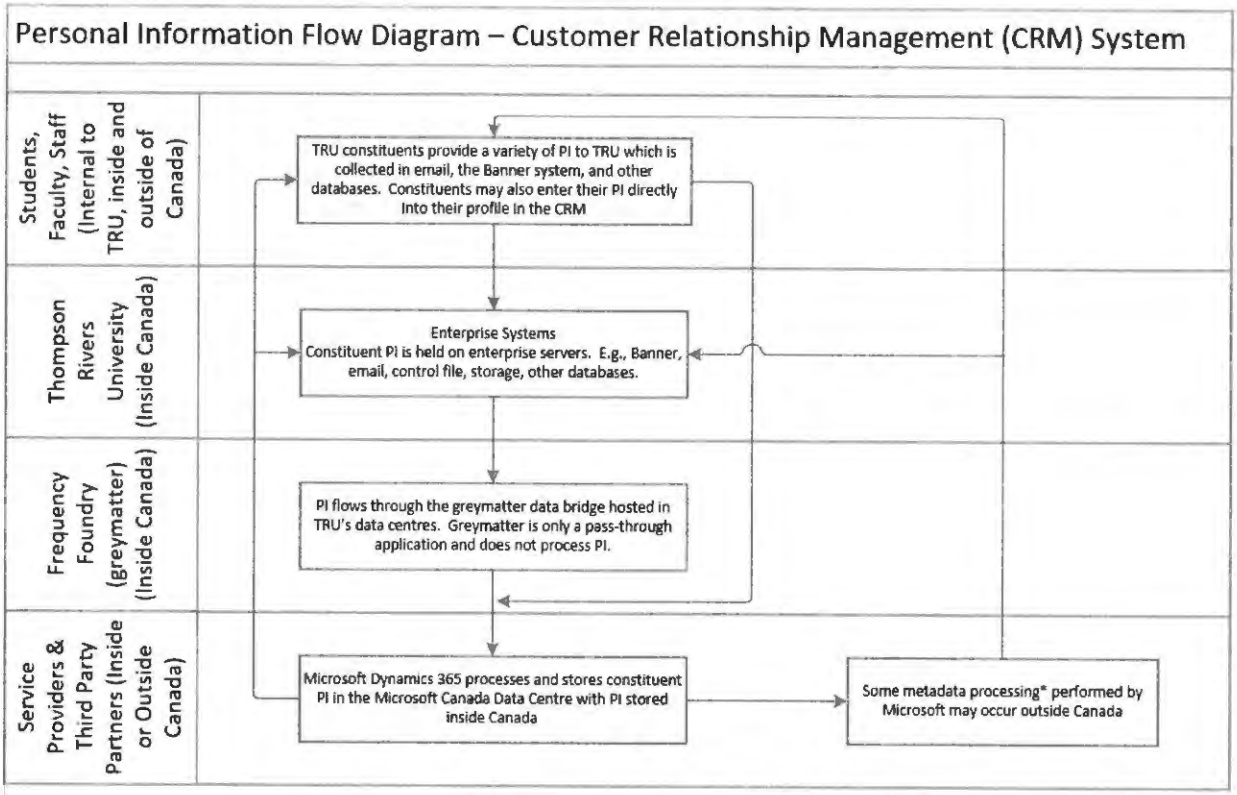
6. Data-linking Initiative*

In FIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	Yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation (a contract/agreement) that meets the requirements set out in the FIPPA regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table



* Examples may include spell check, translation services, artificial intelligence that predicts intent or outcomes, etc. which may be disabled.

FIPPA authorities that allow for the collection, use and disclosure of personal information with the use of the CRM:

Collection of personal information – section 26(c) & 26(e)
Use of personal information – section 32
Disclosure of personal information – section 33.1 & 33.2

9. Risk Mitigation Table (A Listing of Identified Issues and Recommendations for the Project)

Identified privacy risks associated with this initiative along with recommended mitigation strategies are listed in Appendix A.

10. Collection Notice

Collection notifications should be presented to individuals at identified collection points as required under section 26 of the FIPPA. Each collection point may have its own purpose for the collection of personal information and these specific purposes must be included in each required notification.

Collection Notices are different from consents from data subjects; notices are issued unilaterally by TRU and do not authorize TRU to store or allow access to personal information in the custody or control of TRU outside of Canada.

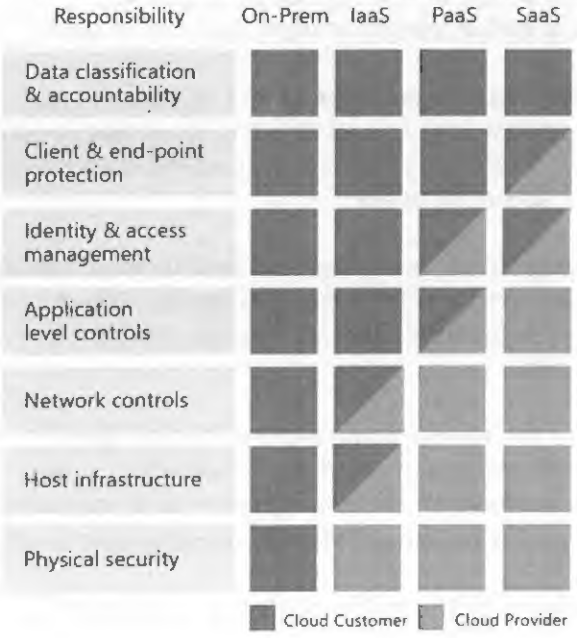
s.13 [redacted]

Part 3 – Security of Personal Information

11. Summary

TRU's Information Security Manager has reviewed Microsoft's information security program and has reported that Microsoft has a very mature and well-defined information security program. Microsoft provides validation through a large number of publicly available external audits that can be reviewed on the Microsoft Trust Center in the Microsoft Azure Compliance Offerings. See Appendix D for links to webpages containing audit reports. These controls are applied to Microsoft Azure and Dynamics. The documentation associated with this program is many hundreds of pages in length and is comprehensive.

Table 4 – Information Security Configuration Responsibilities



s.13 [redacted]

12. Please describe the physical security measures related to the initiative (if applicable).

Microsoft Literature (https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security) indicates as follows (while this Literature is not contractually binding on Microsoft, it is a representation that TRU can take into account in deciding whether TRU is meeting FIPPA section 30):

> *All data is stored in the Microsoft Canada data centres only. Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where our data is stored. Microsoft understands the importance of protecting your data and is committed to helping secure the datacenters that contain our data. Microsoft has an entire division devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.*
>
> *Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:*
>
> - ***Access request and approval.*** *Everyone must request access prior to arriving at the datacenter and are required to provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the datacenters to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the datacenter required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.*
>
> - ***Facility's perimeter.*** *When you arrive at a datacenter, you're required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacenters, with a security team monitoring their videos at all times.*
>
> - ***Building entrance.*** *The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter, and monitor the videos of cameras inside the datacenter at all times.*
>
> - ***Inside the building.*** *After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the datacenter. If your identity is validated, you can enter only the portion of the datacenter that you have approved access to. You can stay there only for the duration of the time approved.*
>
> - ***Datacenter floor.*** *You are only allowed onto the floor that you're approved to enter. You are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the datacenter floor, you again must pass through full body metal detection screening. To leave the datacenter, you're required to pass through an additional security scan.*

Microsoft requires visitors to surrender badges upon departure from any Microsoft facility.

Physical security reviews
Periodically, we conduct physical security reviews of the facilities, to ensure the datacenters properly address Azure security requirements. The datacenter hosting provider personnel do not provide Azure service management. Personnel can't sign in to Azure systems and don't have physical access to the Azure collocation room and cages.

Data bearing devices
Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped, we use a destruction process that destroys it and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. We determine the means of disposal according to the asset type. We retain records of the destruction.

Equipment disposal
Upon a system's end-of-life, Microsoft operational personnel follow rigorous data handling and hardware disposal procedures to assure that hardware containing your data is not made available to untrusted parties. We use a secure erase approach for hard drives that support it. For hard drives that can't be wiped, we use a destruction process that destroys the drive and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. We determine the means of disposal according to the asset type. We retain records of the destruction. All Azure services use approved media storage and disposal management services.

Compliance

Microsoft designs and manages the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. We also meet country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

The URL for a full list of compliance standards that Azure adheres to is attached as Appendix E.

The CRM is entirely hosted in Microsoft's Azure system in the Canadian Microsoft data center (with the Data Bridge hosted on site in the TRU data centre). As such, physical access to the servers and network resources that host this application is restricted to Microsoft personnel. Greymatter personnel do not have physical access to these resources.

13. Please describe the technical security measures related to the initiative (if applicable).

a. Microsoft

Microsoft Literature (https://www.microsoft.com/en-us/securityengineering/sdl/practices) indicates as follows:

> *Microsoft Dynamics 365 is developed using the Security Development Lifecycle (SDL), a mandatory Microsoft process that embeds security requirements into every phase of development. Using the SDL means that software is more secure because the SDL reduces the number and severity of vulnerabilities in code plus helps address compliance requirements. The result is higher security and privacy for enterprise applications and data.*
>
> *The protocol used to transfer data to D365 is HTTPS TLS 1.2.*

There are a very large number of technical security measures involved in this project.

s.13 [redacted]

b. Azure Security Measures

1. Network Security

Operational Security Assurance (OSA) makes the infrastructure of Microsoft cloud-based services more resilient to attack by decreasing the amount of time needed to prevent, detect and respond to real and potential Internet based security threats. It ensures that operational activities follow rigorous security guidelines and validates that these guidelines are followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA support mitigations to address them. Azure monitors and blocks unauthorized traffic to and within Microsoft data centers, using a variety of technologies such as layer 7 technologies, firewalls, partitioned local area networks (LANs) and the physical separation of back-end servers from public-facing interfaces.

2. Azure Threat Management

Microsoft's global incident response team works around the clock to mitigate the effects of any attacks against the security of Azure. The teams are backed by centers of excellence that fight digital crime, respond to security incidents and vulnerabilities in Microsoft software, and Azure's Distributed Denial of Service (DDoS) defense system is not only designed to withstand attacks from the outside, but from other Azure tenants as well. Azure uses standard intrusion detection and

mitigation techniques such as SYN cookies, rate limiting and connection limits to protect against these attacks.

3. Penetration Testing
Microsoft conducts regular penetration testing to improve Azure security controls and processes on their infrastructure.

14. Does your department have any departmental security policies?

TRU Information Security Policies and Standards are overseen by the Information Security Committee and apply across the institution.

15. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

TRU's Access Control Standard will be followed. Access control is covered in the Security Concepts (Appendix G) document and in more detail in the Scalable Security Modeling with Microsoft Dynamics CRM white paper (Appendix H).

16. Please describe how you track who has access to the collected/used/stored personal information for this project.

The CRM system will allow TRU administrators to conduct audits on all accounts. Only administrators with granted role-based security access will be able to perform such account audits. Furthermore, the solution allows identification clean ups to occur on demand, or as per a schedule.

Microsoft Dynamics 365 comes with several tools to help manage data. One of these is the auditing feature, which allows tracking of changes made to data in Dynamics 365. It also tracks each time a user logs into the system. If auditing is enabled, the CRM automatically creates logs for the changes that are tracked. It is expected that these logs will be ported to the current TRU Banner system.

Greymatter allows administrators to conduct audits on all accounts. Only administrators with granted role-based security access will be able to perform such account audits. Furthermore, the solution allows identification clean ups to occur on demand, or as per a schedule.

Microsoft is certified via ISO 27018 Privacy Controls Testing, which ensures the following:

- Access to Customer Data is strictly controlled and logged.
- The event log records access and use of information systems containing Customer Data, registering access ID, time, authorization granted or denied, and relevant activity, regardless of whether the access was granted or denied.
- Microsoft does not disclose customer data in the course of normal operations, except in response to requests that are in compliance with US and International Law.

Part 4 – Accuracy/Correction/Retention of Personal Information

17. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

For some approved data fields, users may update their own information within their profile inside the CRM after authenticating and validating their identity as per existing TRU data standards. These self-serve updates will flow back into Banner (or other systems as permitted) to update the record in that location.

Other data, such as name and birthday will require updating only by approved staff members and will be done in Banner and will be limited by Banner access restrictions. Extensive auditing ensures all changes are audited and no personal information shall be shared outside of TRU.

18. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Yes: TRU will use the information gathered to provide a variety of supports, including but not limited to academic planning, career development, donor management, international agent management, alumni relations, and health and wellness.

19. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

The CRM will adhere to all existing data use policies at TRU. Personal information that will be replicated or directly collected in the CRM will be vetted as to existing departmental and institutional policies and procedures. In addition, as part of the implementation of the CRM, staff will be trained on TRU's data standards and the importance of accurate record keeping. Forms used for data entry can be created using validation for mandatory fields and entry standards (e.g., phone number can only be entered as 123-456-7890).

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Yes, but only to users authorized by TRU.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact the Privacy Office.	

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

Yes. Data may be gathered from the CRM for TRU's own use for statistical purposes.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact the Privacy Office.	

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

Yes. A personal information bank is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Types of Personal Information in the PIB by Constituent group

See Table 3

Authority for Collecting Personal Information

Section 26

Purpose for Which Personal Information is Obtained and Used

See Table 2

Categories of Individuals Using Personal Information or to Whom it is Disclosed

See Table 2

Part 6 – Other Comments

Part 7 – Program Area Signatures

January 20, 2020
Date

s.22 [redacted]
Project Sponsor
Maggie Fung
AVP, Digital Strategies and CIO

January 20, 2020

Date

Matt Milovick
Vice-President, Administration and Finance

s.22 [redacted]

Please date, sign and return.

Appendix A.
Privacy Risk Mitigation Table -

(Risk is assessed using TRU's Risk Assessment Consequence and Evaluation Tables)

# (Risk Category)	Risk/Issue	Likelihood	Impact	Mitigation Strategy/Recommendation	Rationale
1 (Collection)	s.13 [redacted]				
2 (Collection)					

3 (Collection & Use)	s.13 [redacted]
4 (Use)	[redacted]
5 (Use)	[redacted]

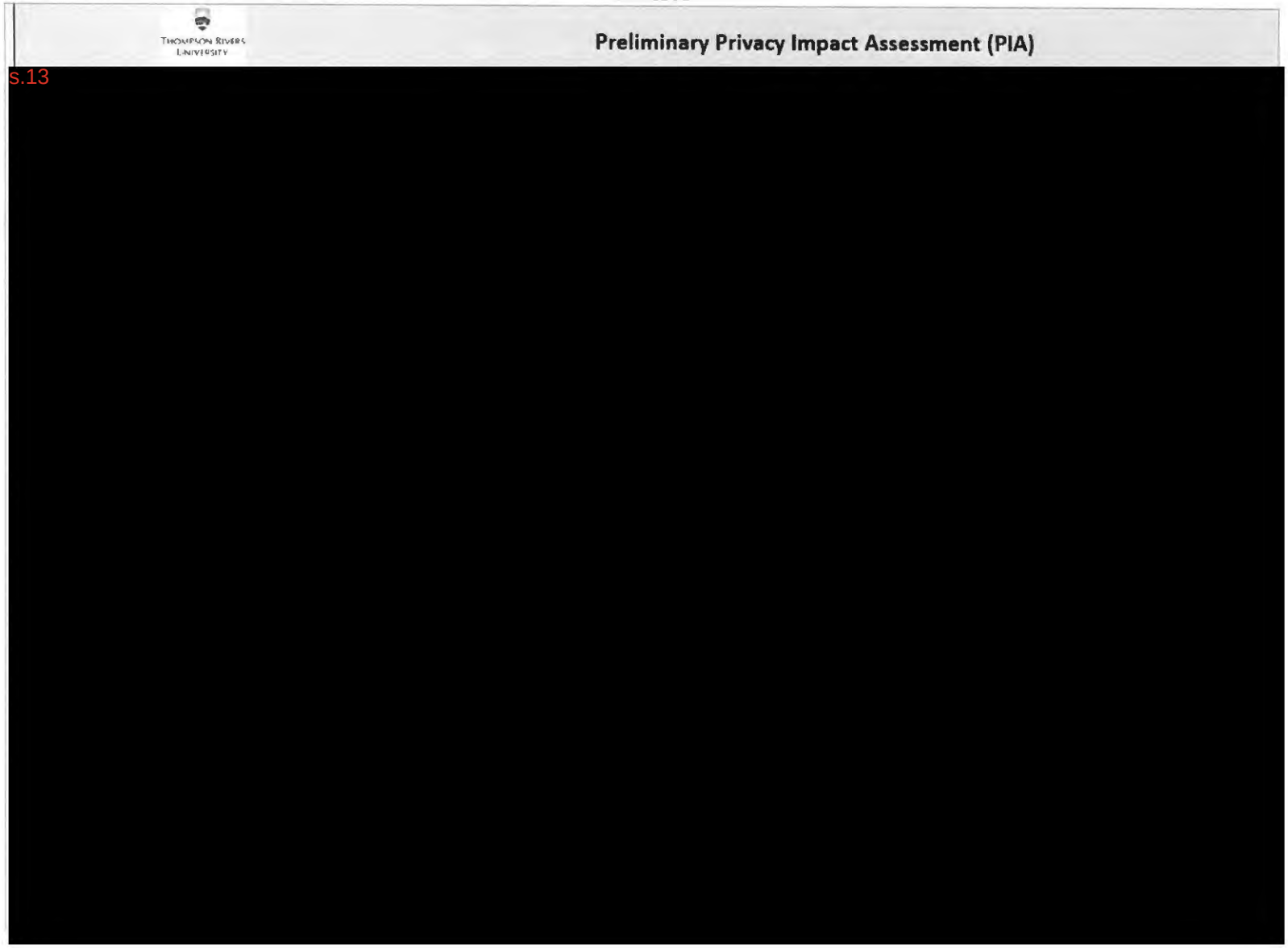
	s.13 [redacted]
6 (Use)	
7 (Use & Disclosure)	
8 (Use & Disclosure)	

9 (Disclosure)	s.13 [redacted]
10 (Disclosure)	[redacted]

11 (Disclosure)	s.13 [redacted]
12 (Disclosure)	
13 (Disclosure)	
14 (Retention)	

				s.13 [redacted]

Appendix B


Thompson Rivers University
Preliminary Privacy Impact Assessment (PIA)
s.13

Appendix C

Dynamics 365 Licensing Guide (July 2019) – 61 pages

https://mbs.microsoft.com/Files/public/365/Dynamics365LicensingGuide.pdf

Appendix D

Microsoft Audits (require Microsoft account to access) – available at

https://azure.microsoft.com/en-ca/overview/trusted-cloud/compliance/

https://www.microsoft.com/en-us/trustcenter/Compliance/soc

https://servicetrust.microsoft.com/Documents/ComplianceReports

Appendix E

Microsoft Azure Compliance Offerings

https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942/file/178110/25/Microsoft%20Azure%20Compliance%20Offerings.pdf

Appendix F

Supporting Your EU GDPR Compliance Journey white paper

http://download.microsoft.com/download/8/1/7/8179EE68-66E0-44C7-BDC7-66443CAC0FF6/EMSandGDPRwhitepaper.pdf

Appendix G

TRU Access Control Standard

https://www.tru.ca/__shared/assets/tru-access-control-standard39325.pdf

Appendix H

Scalable Security Modeling with Microsoft Dynamics CRM white paper

Download from: https://download.microsoft.com/download/D/6/6/D66E61BA-3D18-49E8-B042-8434E64FAFCA/Scalable%20Security%20Modeling%20with%20Microsoft%20Dynamics%20CRM%202015.pdf