PIA01576 – BeyondTrust

PIA REVIEW – EXECUTIVE REPORT

PREFACE

This document forms part of UBC Safety and Risk Services (SRS) PrISM's internal documentation for support and administration of the Privacy Impact Assessment (PIA) Review Process. In particular, it documents the final report of the specified PIA review.

This segment serves to provide and record document control capabilities for this document.

Controlled Document

The template and final report documents are controlled documents. The master electronic versions of each reside on the SRS TeamShare S-drive. Any copies or versions not provided directly by the SRS PrISM team, or which have a broken chain of custody, are not to be considered as official copies.

Document Control

The following sub-sections provide a record of the base document template revision history and control.

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Christian Stockman	Safety and Risk Services	Privacy and Information Security Risk Advisor

Figure 1 - Major Document Revision Approval History

TEMPLATE REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
1.0	2020-10-30	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2020-10-30	Dana Caudle	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

TABLE OF FIGURES

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

Addition of BeyondTrust tenant to UBC Okanagan.

1.2 Description of the Program, System, Application, or Initiative Assessed

UBC Cybersecurity is looking to add a tenant to the UBC Okanagan BeyondTrust solution. This is hosted on-prem at the Okanagan campus. This solution is a vendor-supplied virtual appliance that is used to remotely support users and endpoints. This solution has been used at the Okanagan campus for years, and we are adding a tenant so that Cybersecurity can also make use of this tool.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is **3 - Medium**.
The residual risk classification level of this PIA submission at closure is **3 – Medium**.

1.3 Scope of PIA

Extended use of BeyondTrust solution.

1.4 Related PIAs

There are no directly related PIAs completed within UBC.

1.5 Elements of Information or Data

The remote support may be part of security incident investigations, or it may be to assist users with security-related questions or processes.

While the system itself does not store PI, it does capture screen recordings and chat transcripts of remote support sessions. As a result, those recordings could contain incidental PI if the endpoint being controlled is currently displaying PI on the screen. Recording resolution isn't 1:1, data is compressed and, as a result, it would be difficult to "gather" PI from the recordings.

1.6 Storage or Access Outside of Canada (including back-ups and recovery)

Not applicable, BeyondTrust appliance is hosted at UBC IT Data Center. The appliance is self-contained. Session logs and recordings are stored on the appliance itself. Appliance logs [logins, logouts, changes to policies, etc.] are shipped to the UBC Okanagan Graylog centralized logging service syslog.ok.ubc.ca.

1.8 Data-Linking Initiative

In FIPPA, "data linking" and "data-linking initiative" are strictly defined; if a project is a data linking initiative, it must comply with specific requirements under the Act related to data-linking initiative	
1. *Personal information from one database is linked or combined with personal information from another database;*	**No**
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**
This project/initiative is not considered a data linking initiative as contemplated under s.(36) of FIPPA.	

1.9 Is this a Common or Integrated Program or Activity?

In FIPPA, "common or integrated program or activity" is strictly defined; where one exists it 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);*	**No**
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 that meets the requirements set out in the FIPPA regulation.*	**No**
This project/initiative is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.	

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

Not applicable

2.2 Risk Mitigation Table

Not applicable

2.3 Collection Notice

Not applicable

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

Not applicable.

2.5 Consent Withheld Procedure

Not applicable.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project/initiative is required to comply with UBC Information Security Policy (SC-14roject is required to comply with UBC Information Security Policy (SC-14).

3.2 Technical Security Measures

This project/initiative is required to comply with UBC Information Security Policy (SC-14).

- This software does not open up any direct channels for malware to transmit unrequested onto our systems, as it does not provide direct bridging inside networks to outside networks.
- The software does allow for file transfer, but only if initiated by the Representative. The Client devices cannot initiate a transfer. The Representative can both "push" from the Representative Device to the Client device, and "pull" from the Client Device to Representative Device.
- The only way in which this tool could be used to spread malware onto a Representative Device would be for a Representative to connect to an infected Client Device, intentionally locate a piece of malware, download it to their Representative Device [again, intentionally - we would have to locate the files], and then execute said malware.
- In this case, the Representatives are made up of members from the Cybersecurity team who work with malware on a regular basis, and we do not infect ourselves in this manner. In the case of a highly volatile situation, Cybersecurity staff would be capable of connecting to the Client Device using this tool inside of a local VM environment on the Representative Device.

3.3 Security Policies, Procedures, and Standards

This project/initiative is required to comply with UBC Information Security Policy (SC-14).

3.4 Tracking Access / Access Controls

Session recording access is as follows:

a. Most representatives cannot view recordings at all.
b. Some representatives can view their own recordings only.
c. Team managers will have access to view the session logs of all representatives on their teams.
d. Four BeyondTrust appliance administrators have the ability to view all client recordings.

BeyondTrust appliance administrators are UBC staff responsible for the care and maintenance of the BeyondTrust appliance, and not actually BeyondTrust staff. The appliance does have a feature to allow support personnel from BeyondTrust to assist directly on the appliance. This feature requires that a UBC administrator initiate the request, and such access is only granted temporarily by the technical controls built into the appliance.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not applicable.

4.2 Decisions That Directly Affect an Individual

This project/initiative does not capture personal information that directly affects an individual.

4.3 Records Retention and Disposal

The recordings are kept for approximately 90 days to comply with UBC Information Security Standard.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

The initiative does not involve the systemic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

This project/initiative does not involve the disclosure of personal information for research or statistical purposes as contemplated under s.(35) of FIPPA.

5.3 Other Applicable Legislation and Regulations

This project/initiative is not subject to other applicable legislation or regulations.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

The provided information was deemed reasonable to provide an understanding of operated controls.

6.2 Information or Materials Not Available for Review

Not applicable.

6.3 Analysis and Summary

Based on the information provided, our review has concluded there are no significant privacy or security risks introduced by this Initiative provided the Project Owner complies with the responsibilities outlined.

6.4 Conditions of Approval

None Specified.

6.5 Review and Distribution

This refers to the report approval process. The Owner is accepting the accuracy of the data provided to PrISM for this review and the risk responses. The Owner is responsible for the on-going operational activities and must ensure that this project continues to meet legislative and legal requirements, along with Information Systems Policy (SC14) requirements. Any change in PI collection or use will require new PIA.

Assessment Acceptance
Owner - Aaron Heck

This refers to the report distribution, including Requestor, Project Manager, Owner, and assigned Risk Advisor.

Distributed To
Requestor: Aaron Heck **Project Manager:** Aaron Heck **Owner:** Dana Caudle **Business Approver:** Aaron Heck **Risk Advisor** Pimkae Saisamorn

PIA Request History:

PIA Request Date	Report Created
2020-06-02 13:35:38	2020-11-06 20:06:31