PIA02328 – GitHub

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
Taylor Bohn	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	2023-04-04	Taylor Bohn	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2023-04-04	Anthony Winstanley	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

TABLE OF FIGURES

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Unit and Program Area

The Computer Science department will be hosting GitHub Enterprise environment in EduCloud. The primary purpose of its use will be to collaborate and maintain version control over operational code. "Integrations" with internal systems are done with git clone/pull commands and include but are not limited to Websites, Configuration Management, or Other Administrative tools. Limited external access is required and for this reason all repositories are privacy and no external facing integration/API's have been enabled. The service will be made available to technical staff and researchers. Access to researchers is provided only if their intended use case of the service aligns with the private/internal restrictions applied to the GitHub Environment. Guest may also be provided access to the environment, but access requests will need to be submitted via the established approval process.

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

The intention is to provide an internal Git service for the Department of Computer Science. GitHub is a popular web-based code hosting platform for version control and collaboration. This service will then be used by both staff and faculty, primary use will be for hosting operational code, however access will be extended to researchers if their intended use of the service aligns with the private/internal restrictions applied to the GitHub Environment.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is **4 – High**.
The residual risk classification level of this PIA submission at closure is **4 - High**.

1.3 Scope

The Scope of this PIA will review the computer science departments intended use of their selfhosted GitHub environment. It will establish who will have access to the environment and how they access the environment. Additionally, this review will also cover if any external systems are integrated with GitHub as well as identify if any public facing repositories or aspects with the service.

This scope will not review github.students.cs.ubc.ca as this instance was reviewed under PIA 2018.01-005 and will not review specific use cases for repositories hosted in the GitHub environment.

1.4 Related PIA

PIA 2018.01-005.

1.5 Data Elements

The following user attributes are required for account creation:

First name, Last name, email addresses and CWL.

Since the primary users of the service are staff and/or faculty this information would be considered business contact information. Guest users review the Acceptable Use Policy and provide consent upon submission of their request for access. Additionally, any content users upload/create on the platform will be visible to those who have the required permissions. As stated in the Universities acceptable use policy private or personal business use of the service is deemed to be unacceptable.

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

Not applicable as all the GitHub Environment is hosted in EduCloud, access to the environment is also limited to internal UBC networks.

1.7 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under s.(36) of FIPPA.

1.8 Is this a Common or Integrated Program or Activity?

This project 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 as this system will not contain and personal information.

2.2 Risk Mitigation Table

The following table indicates the associated risk levels as applicable and the potential or intended mitigation steps.

Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Disclosing to or allowing unauthorized users access	RK0021506	4 - High	4 - Major	Mitigate	4 - Low
	Mitigation Plan: Guest accounts may be provided access to the GitHub instances; however, they will be required to go through the required approval process to do so. The link below outlines the acceptable use policy and registration form guests accounts will need to submit to gain access. This request is then reviewed by admins and determined if access is required. https://my.cs.ubc.ca/sites/default/files/docs/accountform.pdf".				

Figure 4 - Risk Mitigation Table

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 is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.4 Tracking Access / Access Controls

By default, users will not be provided access to anything other than their own private repositories. Organizations in GitHub are then used to separate access, Organizations are only created when they have a clear institutional owner. These individuals are then granted ownership access to the organization, and from there decide who will have access to the organization and the ability to view and/or edit repositories associated within the organization. There are a handful of technical-staff site admins with superuser access. Superuser access is always logged.

Users authenticate to the service using CWL credentials, this is made possible by the departments use of ELDAPDC, which is a department-based domain specific to Computer Science. Currently, the suffix only contains the technical staff subset of users from the departments existing local departmental domain. All GitHub accounts are created and managed by IT admins; Guest access may be permitted but approval will need to be submitted. For approval to be accepted guests are required to complete and submit the guest form which can be found using the link below.

https://my.cs.ubc.ca/sites/default/files/docs/accountform.pdf

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not Applicable.

4.2 Decisions That Directly Affect an Individual

Not Applicable.

4.3 Records Retention and Disposal

Account access is dictated by the computer science departments account management system which has set expiry dates for accounts. When an account is no longer "sponsored", it is then deleted system wide. Sponsorships come from various sources, some are tied to UBC Data such as course registration, others come from researchers sponsoring guest accounts. Organization owners are responsible for determining when repositories should be archived and or deleted. In the event the final owner of an organization is deleted, an admin will determine if the organization should be purged or if a new owner will need to be assigned.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

Not Applicable.

5.2 Access for Research or Statistical Purposes

Access to github.cs.ubc.ca will be provided to Computer Science department researchers who request access to use the service, however data regarding the use of github.cs.ubc.ca will not be used for research/statistical purposes.

5.3 Other Applicable Legislation and Regulations

Not Applicable.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

Information Reviewed	Date Received
guestaccountform.pdf	2023-04-04 16:08:25

6.2 Analysis and Findings

The information provided for the review has established that github.cs.ubc.ca can be used in the proposed manner in compliance with FIPPA and UBC's Information Security Standards. The following are the key factors in that determination:

- Information is collected, stored, and accessed within Canada.
- Information is kept secure during transmission and at rest.
- Access for guest accounts has an established approval process.
- Access requires use of a valid login credentials which leverages CWL.

6.3 Conditions of Approval

Not Applicable.

6.4 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
Anthony Winstanley

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

Distributed To
Requestor: Anthony Winstanley, Director of Information Technology (IT)
Project Manager: Anthony Winstanley, Director of Information Technology (IT)
Owner: Anthony Winstanley, Director of Information Technology (IT)
Risk Advisor: Taylor Bohn, Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2022-05-05 14:46:00	2023-04-04 17:48:33