PRIVACY MATTERS
@ UBC

PIA01467 — AppArmor Platform

1.1 Executive Summary

UBC has employed the AppArmor Safety app ("UBC Safe") since May 2018, facilitated by UBCO Campus Security. This app provides the UBC community with essential resources, including emergency services, first aid, and safe walk programs, enhancing campus security and response capabilities.

The PIA was conducted for the Safety app and it was noted that no personal information was collected during the time of the review in May 2018. WorkAlone app, a component of the Safety app, was piloted with UBCV Michael Smith Labs (MSL) in October 2019 due to an urgent business need and ensure it fits for purpose for a wider launch, with an exception of shared mobile device is not permitted. Lastly, Command app has also been in operations and used by UBCV Emergency Management and CMT Communications to facilitate team chat capabilities, auto-dial conference call bridges and searchable crisis contacts and plans. The PIA of WorkAlone and Command apps was not fully conducted since the apps had been launched.

UBC SRS is looking to expand the use of AppArmor with an additional product named Alert app for the Emergency Mass Notification System including SMS, email, voice, push notifications, desktop, digital signage, etc. The Alert app will replace an existing mass notification system named UBC Alert provided by ReGroup.

AppArmor is comprised of two major components: mobile application and portal dashboard. The mobile application is accessed by UBC community and the portal dashboard accessed by UBC key users. The dashboard is used to manage user access administration, emergency notification, real-time and history logs for safety and security services.

The information collected is stored in both mobile devices and database servers the dashboard connected with. AppArmor hosts its servers at Microsoft Azure in Canada location. AppArmor uses Twilio and SendGrid to provide SMS and email mass notifications respectively.

1.2 Project Description and Scope

UBC Safety & Risk Services (SRS) is looking to implement a robust safety and emergency communication system that has easy mobile access to facilitate work alone or in isolation, identify an emergency or incident on campus, initiate responses and inform the UBC community of critical information and appropriate actions to take. AppArmor (a Division of CutCom Software Inc.) founded and based in Toronto is engaged to provide custom branded mobile safety app, emergency notifications app, and crisis responses app. The Emergency Notification System will be available to the entire community on the UBC Okanagan (UBCO) campus, the UBC Vancouver (UBCV) campus and surrounding neighborhood - University Neighborhood Association (UNA). The Safety app will be available to all students, faculty, staff and community members with a subset having access to the Work Alone app functions.

The project is currently in the development phase, with ongoing documentation based on the latest discussions and information. Details provided here are preliminary and subject to future updates to ensure continual alignment with project goals and compliance requirements.

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 Risk Mitigation Table

Privacy Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
PI stored / accessible outside of Canada	RK0020199	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: To better align with data sovereignty requirements: Enhanced measures are being implemented to ensure that personal information remains within Canada, except as strictly necessary for system functionality, in compliance with FIPPA regulations.				
Retaining PI longer than necessary	RK0020200	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: **All** - The Project implement records retention requirements for transitory records in collaboration with the UBC Records Management Office. The followings are examples of information captured need retention schedules: • AppArmor Dashboard contains a number of history logs including WorkAlone Session history log, Chat history log, Alert Status Archives, Voice/SMS/email history log, Walk History records, Incident Reporting log, etc. • Local mobile device contains all chat history.				
Weak or absence of retention controls	RK0020201	3 - Medium	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: **All** - Each individual be granted access to the AppArmor Portal Dashboard based on their roles and responsibilities and on a need-to-access basis. Security access matrix and group permission should be utilized for easy maintenance.				
Disposing of personal information using inadequate methods	RK0020202	3 - Medium	4 - Major	Mitigate	4 - High
	Mitigation Plan: **Alert app** - A data destruction plan for Regroup be made available and followed the UBC's destruction guideline.				
Not ensuring informed PI sharing with third parties	RK0020203	4 - High	4 - Major	Mitigate	4 - High
	Mitigation Plan: **Alert app** - An existing information sharing agreement between UBC and UNA be updated to reflect the prevailing information and arrangement.				
Not ensuring individuals are informed about collection	RK0020205	4 - High	4 - Major	Mitigate	4 - High
	Mitigation Plan: **Alert app** - The existing collection notice for UBC Alert to send SMS and email notifications posted on the UBC HR System (MSP/WorkDay) and the Student Information Service Centre (SISC) be revised and placed at the right location.				
Disclosing to or allowing unauthorized users access	RK0020206	4 - High	4 - Major	Mitigate	4 - High
	Mitigation Plan: **WorkAlone app** -Enforce access authorization and authentication by implementing the CWL integration at a mobile application layer.				
Use of PI for alternate purpose	RK0020207	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: **WorkAlone app** - To prevent use of information collected to improve worker safety for other purposes, e.g., monitoring attendance, communications must be developed and integrated with the app and work alone training to inform the user community of appropriate and inappropriate use of work alone information.				

Security Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of technical security controls	RK0020204	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: **Alert app** - Data stored on the FTP server been crypted using AES256 in accordance with the UBC Information Security Standard. Noted during the course of the review that the AES 256 encryption has been implemented on the data stored on the FTP server.				

1.4 Information Reviewed

Document review comments: The information provided to-date was deemed reasonable to provide an understanding of operated controls.

Documents not available for review: Not applicable.

1.5 Analysis and Findings

Our review has highlighted certain privacy and security concerns that are comprehensively addressed in the risk mitigation section. We recommend that the project team thoroughly review and implement the necessary risk mitigation plans to effectively manage and mitigate identified risks before advancing with the implementation of AppArmor. This proactive approach will safeguard the integrity of UBC systems and the confidentiality of personal and third-party information.

1.6 Conditions of Approval

Given this is a mid-phase of the project and the PIA review will continue to carry on, it is acceptable for the project to proceed with the development and provided that the observations as described in the above section are to be addressed. As the review is moving along, the project can expect additional questions, information requests, and/or observations which may be discovered during the course of the PIA review.

1.7 Review and Distribution

The Minister of Citizens' Services Direction 2-21, *Privacy Impact Assessment Directions* requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s. D8).

Accountability is maintained by the role or position, regardless of who fills the role.

Under UBC Policy SC14, Administrative Heads of Unit are responsible for:

- ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
- ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
- authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
- renewing, retiring, and revoking User authorizations within their area of responsibility.

Holding accountability for the privacy risks of this initiative includes:

- reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;
- ensuring accountability is transferred to any individual who assumes this role;
- if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the PIA team is engaged, and if necessary, completing a PIA update; and
- understanding what your privacy obligations are, and if not, following up with the PIA team.

Assessment Acceptance
RaeAnn Aldridge

Distribution
Requestor: Danny Smutylo **Project Manager**: Faiza Samnani **Owner**: RaeAnn Aldridge **Risk Advisor**: Pimkae Saisamorn

PIA Request Submission	Report Completion
2020-06-02	2020-10-07