University of Victoria

License Plate Recognition (LPR) Privacy Impact Assessment

Project Code	PC0662
Submission Date	December 5, 2016
Organization	University of Victoria
Unit and Service Owner	Campus Security Services
Contact	Patrick Seward, Manager, Parking & Transportation. Parkingmgr@uvic.ca Local 6685
Reviewed By	Bill Trott, Chief Privacy Officer
Review Date	

1.0 Privacy Context

1.1 Description of Systems and Linkage to Legislation

[[Describe the systems being implemented or changed as a result of this project, and what implications there are in terms of FIPPA.]]

The Automatic License Plate Recognition System (ALPR) utilizes a vehicle with an on-board computer and rooftop-mounted cameras to scan and photograph license plates in a geographic area. A photograph is taken when a license plate is detected, and the license plate photo is converted into data format. This data is cross-referenced with permit-holder data (license plate number/province, permit number, timestamp data) that has been securely uploaded to the on-board computer (laptop) from the existing Sec. 15 The Sec. 15 will then query the Sec. 15 in Burnaby as a final check to determine if the suspected vehicle has purchased parking in the last few moments. Permit-holder information is periodically updated throughout the day via the same secure connection, encrypted, to ensure permit-holder information on the laptop remains current. All data and photos on the laptop are automatically deleted at the end of the day via the vendor's proprietary process, when the data is downloaded to the Sec. 15 The data in the Sec. 15 will be immediately deleted as it is not needed.

When a violation is detected, the officer issues a citation via the existing citation process.

The existing citation process involves an officer manually entering citation data onto an app on an iPhone dedicated for this purpose, taking a photo of the license plate and a wider-angled photo of the entire vehicle, attaching the photos to the citation, and securely downloading the citation and photos to the Sec. 15 The citations and associated photos are stored in the Sec. 15 at UVic indefinitely, which is the existing process.

Implications regarding FIPPA would be the capture of data that can be directly linked to a registered owner, as well as location and duration of data storage, and security of data during transmission.

As part of the next phase of the project, Implementation, Campus Security (CSEC) will be consulting with various areas on campus to advise the community of the technology being implemented, in an effort to allay privacy concerns. Signage will be erected on campus in affected areas to advise of the technology being utilized for parking enforcement.

1.2 Use of System

ALPR Process:

The ALPR system will be used to manage parking enforcement, to ensure that vehicles parked on the Gordon Head Campus have a valid permit, have paid for parking and are not currently suspended from parking on campus. The system will be operated by a Security Officer and operate through cameras mounted on a vehicle, that would scan vehicle license plates in parking lots on campus. Data will only be retrieved for the purpose of managing parking on campus by authorized Campus Security personnel.

Data (License Plate information, province, permit number, expiry date/time information) from the Sec. 15 Permit Database) for valid permit holders, as well as from the Sec. 15 when this functionality is enabled in the future, will be downloaded encrypted via 3G to an encrypted laptop located in the vehicle. A server in the UVic datacenter called Sec. 15 runs core software Sec. 15 that sets up

communication between the Internal Sec. 15 and External Sec. 15 Plate database housed in Burnaby BC) parking databases and the vehicle laptop. Permit-holder information is periodically updated throughout the d y via the same secure connection, to ensure permit-holder information on the laptop remains current.

Two cameras will be mounted on the patrol vehicle. The vehicle will drive through parking lots on the UVic campus. One camera takes a picture of only the license plate, the second has a wider lens which captures an image of the entire vehicle. The photo of the license plate is converted into data. Photos are transmitted to the laptop only when the camera processing unit has analyzed a photo and a license plate is detected. The cameras are activated and disabled manually, and will be manually disabled when not actively in use within parking areas. This procedure will form part of procedure that will be put in place for all users of the equipment

The license plate is converted into data so that it can be read, and is cross-referenced with the permit-holder information on the laptop to determine if a vehicle has a valid permit. When Pay-By-License-Plate is enabled, the laptop will query the Sec. 15 database Sec. 15 , as a final check to verify if the vehicle owner has just purchased parking in the last few moments. If there are no valid parking permits associated with a vehicle, the vehicle is deemed to have committed a parking infraction.

There are four types of data collected in the vehicle using the camera system:

Hits/Hit photos: Data associated with an infraction. The types of hits are: Accepted and enforced, Rejected hits, Accepted but not enforced.

Read/Read photos: data not associated with infraction.

Both Hits and non-hits have a photo associated with it.

If an infraction is detected, the Campus Security personnel driving the vehicle accepts the violation, and issues a citation via the existing citation process, which is a completely separate, pre-existing process.

Sec. 15

Campus Security will not be utilizing the system outside of parking zones. The laptop is designed and will be used solely for the purpose of issuing citations, it will have no additional functionality contained within it, and additional functionality cannot be added to it. The laptop will be secured within the vehicle. The cameras will be manually powered down when not in use and only utilized in parking areas. Information contained on the laptop will be encrypted, and encrypted in transit. The laptop can only be serviced by the vendor, as it is proprietary technology, so all data and photos on the laptop will be deleted by Campus Security before any service can occur. The vendor will not have access to service the laptop remotely.

Existing Citation process:

When the Officer finds a vehicle in violation, the officer enters the infraction information on the Enforcement app on an iPhone dedicated to the citation process. Infraction information includes License Plate Number, colour, style (convertible, van, etc), make, model, violation, location, date/time

The officer takes a photo of license plate and a photo of the vehicle, attaches the photos to the citation, and uploads the citations encrypted to Sec. 15

Sec. 15 pulls data every 2-6 weeks, a list of license plates related to unpaid citations. A Campus Security (CSEC) officer manually uploads the data file to Sec. 15 Sec. 15 using CSEC's ID and Password. Sec. 15 processes the information and deposits a file with information about those vehicles to Sec. 15 . CSEC logs in and receives the data file, prints it, and manually inputs the information into the Sec. 15 Information received from Sec. 15 Vehicle Owner Name, address, postal code. CSEC stores printed copies in a locked filing cabinet, and deletes electronic copy immediately after manual entry.

CSEC then sends emails if they have an email address for the violator, or letters if only a home address.

iPhone control/security is addressed in section 1.3, Record Management, Manual citation system (iPhone)

1.3 Custody and Control

[[Describe what records will be under the possession or use of the institution or system and how the records will be managed to address FIPPA.]]

Records in custody and control of the University include:

1. *Permit data*:

Data from the Sec. 15 nd external Pay by Plate Provider (License Plate number, province, permit number , expiry date/time information) will be uploaded to a laptop located in the vehicle.

2. *ALPR Data*:

There are four types of data collected from parked vehicles via camera. Retention schedules for each type of data can be configured separately, these rules are laid out in the Risk Table item #9 .

Hits/Hit photos: Data associated with an infraction.

Read/Read photos: data not associated with an infraction. The types of hits are: Accepted and enforced, Rejected hits, Accepted but not enforced.

Image of license plate, image of vehicle, date/time of infraction and GPS are retained for as long as laptop is active that day, then automatically scrubbed when the data is downloaded encrypted to Sec. 15 at the end of each day.

Permit-holder information is periodically updated throughout the day via the same secure connection encrypted, to ensure permit-holder information on the laptop remains current.

3. Manually input into enforcement app:

License Plate Number, Colour, Style (convertible, van, etc), Make, Model, Violation info, Location, Timestamped by app. Photos associated with a violation (license plate/entire vehicle)

4. *File uploaded manually to* Sec. 15 *by CSEC*: BC License Plate information

5. *File received from ICBC manually downloaded from* Sec. 15 *by CSEC*: Vehicle Owner Name, mailing address with postal code

Record Management:

ALPR:

Communication between the Vehicle laptop and the Sec. 15 will be encrypted.

The laptop is designed and will be used solely for the purpose of issuing citations, it will have no additional functionality contained within it, and additional functionality cannot be added to it. The laptop is itself encrypted, will be secured within the vehicle, and at the end of the day will be removed from the vehicle and stored in the Campus Security Facility. The cameras will be manually powered down when not in use and only utilized in parking areas. Information contained on the laptop will be encrypted.

Manual Citation system (iPhone):

Sec. 15 extracts data and creates a file with a list of license plates every 2-6 weeks. A CSEC officer manually uploads the data file to a protected folder on Sec. 15 to CSEC's ID and Password. Sec. processes and deposits a return file with information on those vehicles to a return folder on Sec. 15 CSEC logs in and receives the data file, prints it, and manually inputs the information into Sec. 15 Information sent from Sec. Vehicle Owner Name, address, postal code. CSEC stores printed copies in locked filing cabinet, and deletes the electronic copy immediately after manual entry.

1. The iPhone only has the Sec. 15 on it, and the camera enabled. The iPhone is locked down, preventing officers from installing any other apps. Web browsing is locked down.
2. Security on the iPhone: The phone is password protected. Only the individual officers know the password to their individual iPhone (with the Manager of Parking and Transportation knowing everyone's). The Enforcement app itself also has a separate log in and password for each officer.
3. When a citation is issued on the app, the officer takes a photo of the car, attaches it to the file, and the information is sent encrypted via Sec. 15 The data does not leave UVic.
4. The photos are taken within the Enforcement application and do not remain on the device. Within the app, photos are not accessible once the citation is printed, as the data is transmitted to Sec. 15 and automatically wiped from the app.
5. Within Sec. 15 the data exists as part of the citation record and are not deleted. The vendor will be engaged and a request will be made for this functionality.
6. iPhone Software updates are handled by the Manager of Parking and Transportation. The app store is password protected so there is no access by others. When the phones break (they are quite new) CSEC would wipe and dispose of it securely as required to and buy a replacement phone.
7. If the phone needs to be serviced, it will be serviced the same as any other UVic issued phone.
8. If the phone is lost/stolen, the officer would notify CSEC, enable 'find my iPhone' on the phone of either the Manager of Parking and Transportation or the Director of Campus security, and find it or remote wipe it.

1.4 Personally identifiable information Data Types and Information Flows

[[Enumerate all personally identifiable information (PII) data types stored in and accessed by the systems, and how these data types will flow in and out of the systems.]]

ALPR: Permit-holder Data (License Plate information, province, permit number, expiry date/time information) from the UVic Sec. 15 as well as from the external Sec. 15 will be downloaded encrypted to a laptop Sec. 15 A server in Sec. 15

Centre runs core software that sets up communication between the Sec. 15 Sec. 15 and Sec. 15 parking databases, and the Sec. 15 Sec. 15

Two cameras will be mounted on the patrol vehicle. The vehicle will drive through parking lots on the UVic campus. One camera takes a photograph of only the license plate, the second has a wider lens which captures an image of the entire vehicle. Photos are transmitted to the laptop only when the camera processing unit has analyzed a photo and a license plate is detected. The cameras are activated and disabled manually.

The license plate is converted into data so that it can be read, and is cross-referenced with the permit-holder information on the laptop to determine if a vehicle has a valid permit. When Pay-By-License-Plate is enabled at the same time as ALPR, th Sec. 15 , as a final check to verify if the vehicle owner has just purchased parking in the last few moments. If there are no valid parking permits associated with a vehicle, the vehicle is deemed to have committed a parking infraction, and a citation is issued via the existing citation process.

Citation process:

Manually input into enforcement app: License Plate Number, Colour, Style (convertible, van, etc), Make, Model, Violation info, Location, Timestamp by app, Photos. Information is uploaded via Sec. 15 Sec. 15

File uploaded manually to Sec. 15 **by CSEC:** BC License Plate information for vehicles receiving citations

File received from Sec. 15 **manually downloaded from** Sec. 15 **by CSEC**: Vehicle Owner Name, mailing address with postal code

Dataflow Diagrams

FOI2024-017 - 2016

ADD ENCRYPTED OVER WIFI/3G TO ALL WIFI/3G references

2.0 Privacy Threshold Analysis

1	Has a Privacy Impact Assessment ever been performed for this project or program?	[N] [Date]
2	What is the information classification level of information collected, maintained, or shared in any identifiable form as part of this project or service? Select all classification levels that apply. See University Policy IM7800 for detailed definitions. ☐Highly Confidential ☒Confidential ☐Internal ☐Public ☐Don't know ☐Information is not collected, maintained, or shared in any identifiable form as part of this project or service	
3	What are the type(s) of personal, critical, or sensitive information collected, maintained, or shared by this project? Please be specific about the data elements. *Examples include, but are not limited to information about students, employees, donors, alumni, credit cords, health Information, etc. See Appendix A of University Policy IM7800 for more examples.* **Highly Confidential** • [[Add a new bullet point for each data element]] **Confidential** • Personal Vehicle Information (License Plate number/province, permit number, vehicle photo) **Internal** • **Don't Know** •	
4	Does this project or program involve the implementation of a new electronic system or use of a new application/ software to support the creation, collection, storing, backing-up or disposition of personal, sensitive, or critical information?	YEs
5	Does the project apply new or additional information technologies that have substantial potential for privacy intrusion? Cameras mounted on vehicle taking photos of license plates and vehicles in parking areas	Yes
6	Will the project involve the collection or creation of new information about individuals? photos of license plates and vehicles in parking areas	Yes
7	Will personal information about individuals or sensitive/critical information be disclosed to organizations, programs, processes or people who have not previously had routine access to the information? [[If so, which organizations, processes or people?]]	No
8	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? License plate information and permit number in existing Sec. 15 will be uploaded to a vehicle laptop for cross reference with license plate information for the purpose of determining parking infractions.	Yes
9	Will the project collect, use, or disclose PII or sensitive/critical information for research purposes?	No

	[[If so, do you have appropriate research approvals (e.g. ethics)?]]	
10	Will the project require that individuals are contacted in ways that they may perceive to be intrusive? [[If so, how may they perceive it to be intrusive?]]	No
11	Is any of the information owned by another organization? [[If so, which organization(s)?]]	No
12	Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources? [[If so, which ones?]]	No
13	Does this project collect, access or use Social Insurance Numbers (SIN)?	No
14	How many user records containing PII or sensitive/critical information will be stored, accessed or used? [1-1000],[1001-5000],[5,001-50,000],[50,001-100,000],[100,000+]	Sec. 15
15	Where will the information be stored? Laptop located on vehicle	
16	Will a third party (e.g. vendor or service provider) have access to the information? [[If so, which third parties?]]	No
17	Is any of the information being accessed from outside of Canada? [[If so, by whom and from where?]]	No
18	Does the IT system connect, receive, or share information in identifiable form, or PII or sensitive/critical information with any other IT systems? [[If so, which ones? 1. Personal information is transferred to a portable device (laptop computer) 2. Personal information is transmitted using wireless technologies, 3G	Yes
19	If there is external sharing, is it pursuant to new or existing information sharing agreements? [[List these agreements]]	NA

FOI2024-017 - 2016

3.0 Privacy & Security Risks

[[Based on the sections 1.0 and 2.0, determine the probability, impact, and resulting risk score for each of the following risks. Cite the appropriate privacy and security controls from Appendix A and B in your Risk Mitigation Measures and add to the Response section as appropriate. Probability and impact are rated on a scale of 1-5, with 1 representing a small probability or impact and 5 representing a large probability or impact.]]

ID	Risk Description	Probability (1-5)	Impact (1-5)	Risk Mitigation Measures (reduce probability and/or impact)
1	Lack of legal authority to collection, use or disclose PII	1	5	Cars parked on campus, in parking lots, data currently exists within database and used under licence from source Sec. 15 is involved in existing citation process, will not be otherwise involved in the new Sec. 15 process. Under Section 27 Section 1 X.1, the BOG has the authority to impose and collect penalties. This was strengthened in 2010 and specifically allows universities in BC to have regulations that impose fines for Citations, as well as overdue books etc. The link is below: http://www.bclaws.ca/civix/document/id/consol21/consol21/00_96468_01#section71 Privacy Control **AP-1** **Response:** GV0235 Protection of Privacy Policy, section(s) 18.00, 19.00 Privacy Control UL-1 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00 Privacy Control – UL-2 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00
2	Unauthorized collection of PII by authorized individuals/processes/systems	1	3	The system would only operate and collect licence plate numbers of vehicles parked in public areas on campus. Camera will be manually disabled and will not collect images when not in a public area being monitored. Signage will be placed in affected areas advising of the use of this technology. Privacy Control AP-2 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 16.00, 17.00

FOI2024-017 - 2016

				Privacy Control IP-1 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 18.00 Privacy Controls IP-4 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 34.00 Privacy Control UL-1 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00
3	Excessive collection of PII by authorized individuals/processes/systems	1	1	ALPR: Collection would only be done for vehicles parked in public areas on campus, only for parking management. Cameras focus on vehicle license plates, not the surrounding area. Cameras are disabled manually when not in use. Citation via iPhone: iPhone only contains camera and Enforcement App. Only required citation data can be entered. Citations with photos are automatically deleted when citation data is downloaded to Sec. 15 Privacy Control: DM-1 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 19.00 Privacy Control: IP-1 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 18.00

4	Inappropriate or unauthorized use of PII by authorized individuals/processes/systems	1	3	Campus Security sets up all access to the system, ensuring those that need to have access have a unique login id and password, and de-provision users immediately who no longer require access.
				
				Privacy Control: DM-3
				Control(s) / Compliance: GV0235 Protection of Privacy Policy, section(s) 20.00, 21.00, 22.00
				Privacy Control AC-2
				Response:
				• Account Management is governed by the following institutional policies and procedures:
				  • IM7200 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf
				  • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf

FOI2024-017 - 2016

				• Account Management is subject to the operating procedures and processes of the University.
				
				Security Control PL-4
				Control:
				• Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
				• Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
				• Reviews and updates the rules of behavior; and
				• Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated
				
				Security Control AT-2
				Security Awareness Training
				Control:
				• The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
				  • As part of initial training for new users;
				  • When required by information system changes; and
				  • Organization-defined frequency thereafter.
				
				Response:
				• Privacy training will be required for new users to ensure compliance with FIPPA.
				
				IA-2
				Identification and Authentication (organizational Users)
				Control:
				• The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
				
				Response:
				• See SC-8

				Security Response PE-3 **Physical Access Control** **Control:** • Enforces physical access authorizations, controls and audits exist. **UL-2 Information Sharing with Third Parties** Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00,
5	Unauthorized disclosure by individuals/processes/systems	1	3	Sec. 15 Security Control AC-3, AC-4, SC-7 **Control:**

FOI2024-017 - 2016

Sec. 15

Security Control AC-19

Access Control for Mobile Devices

Control:

- Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
- Authorizes the connection of mobile devices to organizational information systems

Response:

- University of Victoria recommends for all users and requires for Exchange users the use of:
  - an encrypted mobile device
  - a password protected mobile device

Privacy:

UL – 1 Use Limitation

Internal Use

The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Control(s) / Compliance:

GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00

				Privacy: UL-2 **Information Sharing with Third Parties** Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00,
6	Creation of new PII by data matching	1	2	ALPR: Information would only be matched to existing information or Sec. 15 Sec. 15 collected for parking management. The only new data created is photos of vehicles and license plates, which are not retained. Citations via iPhone: Existing process. Data is not shared with third parties, with exception of law enforcement if required by law. Security Control SI-12 **Response:** Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf
7	Unauthorized tracking of individuals through transaction monitoring	1	3	Data not retained or transmitted or shared via this technology. Citations and associated information are created by existing system and workflow and kept according to existing procedures. This technology is only utilized for parking enforcement on campus and does not feed into any other systems. Data is not shared with third parties, with exception of law enforcement if required by law.

FOI2024-017 - 2016

				Security Control SI-12 **Response:** Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf
8	Data stored outside of Canada and in the public cloud	1	4	Sec. 15 Sec. 15 Security Control AC-4 **Control:** • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; • Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
9	Data retention beyond prescribed timeline	1	1	1. System would be configured to purge data on a prescribed schedule. The laptop automatically purges all data at the end of day via proprietary software. The data on the laptop is uploaded manually encrypted securely at the end of each day to the Sec. 15 Sec. 15 and immediately manually deleted. 2. There is no retention of images on the iPhone. 3. There is currently no ability to purge data from the Sec. 15 The vendor will be engaged and a request will be made for this functionality. Hit data rule: TBD eg: 24 hours

				Hit photo rule: TBD eg: 24 hours Read data rule: TBD eg: 24 hours Read Photo rule: TBD eg: 24 hours Privacy Control DM-2 **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 20.00, 25.00 Security Control SI-12 **Control:** • The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements **Response:** • Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf
10	Risk of increased surveillance	5	2	Mitigation: ensure configuration values accurately reflect retention rules documented in PIA. Data will be used for parking enforcement purposes only. Data from the laptop will be securely downloaded at the end of the day because it is functionally required, but will be immediately manually deleted. See Retention rules in Risk 9. Privacy Control AP-2 **Purpose Specification** The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

FOI2024-017 - 2016

				Control(s) / Compliance: GV0235 Protection of Privacy Policy, section(s) 16.00, 17.00
11	Unauthorized use as a records repository	1	3	ALPR: System automatically scrubs all data from laptop at end of day (configurable as soon as it's data is securely downloaded encrypted at the end of each day to the Sec. 15 This data is manually deleted from the Sec. 15 mmediately following download. No other data can be stored on the laptop, the laptop is specifically for use for the purpose of parking enforcement. Citation process via iPhone: Citations and attached photos are automatically deleted when citations are downloaded to Sec. 15 **Control:** • The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements **Response:** • Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf
12	Public perception	1	4	Public may see this as increased enforcement activity, or invasion of privacy. Mitigated via consulting with/informing UVic public in advance and responding to concerns, and adding signage in parking areas advising of this monitoring activity. Security Control PL-4 **Control:** • Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

FOI2024-017 - 2016

				• Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; • Reviews and updates the rules of behavior; and • Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated

13	Use of existing PII data in a new system or business process	5	1	The Sec. 15 will only flag violations, it will not act upon them. Citations will continue to be issued using the current process – a handheld device.
				
				Security Control AC-20
				
				Use of External Information Systems
				
				Control:
				
				• The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
				  • Access the information system from external information systems; and
				  • Process, store, or transmit organization-controlled information using external information systems.
				
				Response:
				
				• See CP-9, PE-3, SC-7, SI-8

FOI2024-017 - 2016

Appendix A – Privacy Controls

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	**Authority to Collect** The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. **Response:** GV0235 Protection of Privacy Policy, section(s) 18.00, 19.00
AP-2	**Purpose Specification** The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 16.00, 17.00
DM	Data Minimization and Retention
DM-1	**Minimization of Personally Identifiable Information** Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 19.00
DM-2	**Data Retention and Disposal** Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records). **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 20.00, 25.00
DM-3	**Minimization of PII Used in Testing, Training, and Research** Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and Implements controls to protect PII used for testing, training, and research **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 20.00, 21.00, 22.00
IP	**Individual Participation and Redress**

FOI2024-017 - 2016

ID	PRIVACY CONTROLS
IP-1	**Consent** Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 18.00
IP-2	**Individual Access** Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 29.00, 32.00
IP-3	**Redress** Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 30.00, 31.00, 33.00
IP-4	**Complaint Management** The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 34.00
SE	**Security**
SE-1	**Inventory of Personally Identifiable Information** Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.

FOI2024-017 - 2016

ID	PRIVACY CONTROLS
SE-2	**Privacy Incident Response** Develops and implements a Privacy Incident Response Plan; and Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, Procedures for responding to a Privacy Incident or Privacy Breach
UL	**Use Limitation**
UL-1	**Internal Use** The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00
UL-2	**Information Sharing with Third Parties** Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00,

FOI2024-017 - 2016

ID	SECURITY CONTROLS

AC-2	**Account Management**
	
	Control:
	
	• Identifies and selects the following types of information system accounts to support organizational missions/business functions: organization-defined information system account types;
	• Assigns account managers for information system accounts;
	• Establishes conditions for group and role membership;
	• Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
	• Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
	• Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions;
	• Monitors the use of information system accounts;
	• Notifies account managers:
	  • When accounts are no longer required;
	  • When users are terminated or transferred; and
	  • When individual information system usage or need-to-know changes;
	• Authorizes access to the information system based on:
	  • A valid access authorization;
	  • Intended system usage; and
	  • Other attributes as required by the organization or associated missions/business functions;
	• Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
	• Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
	
	Response:
	
	• Account Management is governed by the following institutional policies and procedures:
	  • IM7200 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf
	  • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf
	• Account Management is subject to the operating procedures and processes of the University.
	
	[[Add additional relevant information as required.]]

AC-3	**Access Enforcement** **Control:** • The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **Response:** • See AC-4, SC-7 [[Add additional relevant information as required.]]

ID	SECURITY CONTROLS
AC-4	**Information Flow Enforcement** **Control:** The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies. **Response:** • See SC-7 [[Add additional relevant information as required.]]

AC-8	**System Use Notification**
	
	Control:
	
	Displays to users an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
	
	Response:
	
	• Organization-defined systems use policy will:
	  • Primarily positive and explanatory (and not just a list of "don'ts").
	  • Encourage usage by providing positive examples and suggestions.
	  • Require that content be office-appropriate.
	  • Require that personally identifiable information is not used.
	  • Include links to University of Victoria policies and training resources
	
	• Organization-defined systems use policy will include reference to and compliance with:
	  • IM700 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf
	  • GV0235 – Protection of Privacy http://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf
	  • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf
	  • IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf
	  • Canadian Copyright Act http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-42/latest/rsc-1985-c-c-42.html
	
	[[Add additional relevant information as required.]]

AC-19	**Access Control for Mobile Devices**
	
	Control:
	
	• Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
	• Authorizes the connection of mobile devices to organizational information systems
	
	Response:
	
	• University of Victoria recommends for all users and requires for Exchange users the use of:
	  • an encrypted mobile device
	  • a password protected mobile device
	  • device wipe on failed login attempts
	
	[[Add additional relevant information as required.]]

FOI2024-017 - 2016

ID	SECURITY CONTROLS

AC-20	**Use of External Information Systems**
	
	Control:
	
	• The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
	  • Access the information system from external information systems; and
	  • Process, store, or transmit organization-controlled information using external information systems.
	
	Response:
	
	• See CP-9, PE-3, SC-7, SI-8
	
	[[Add additional relevant information as required.]]

AC-21	**Information Sharing** **Control:** The organization: • Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required and • Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. **Response:** • See AC-20 [[Add additional relevant information as required.]]
AC-22	**Publically Accessible Content** **Control:** The organization: • Designates individuals authorized to post information onto a publicly accessible information system; • Trains authorized individuals to ensure that publicly accessible information dees not contain nonpublic information; • Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and • Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered. **Response:** • See AC-4, AC-21, IA-2, IA-8 [[Add additional relevant information as required.]]

AT-2	**Security Awareness Training**
	
	Control:
	
	• The organization provides basic security awareness training to information system users (including managers, senior executives, and confractors):
	  • As part of initial training for new users;
	  • When required by information system changes; and

FOI2024-017 - 2016

ID	SECURITY CONTROLS
	• Organization-defined frequency thereafter. **Response:** • Privacy training will be required for new users to ensure compliance with FIPPA. [[Add additional relevant information as required.]]
AU-6	**Audit Review, Analysis, and Reporting** **Control:** The organization: • Reviews and analyzes information system audit records for indications of defined inappropriate or unusual activity. • Reports findings to the Chief Privacy Officer and Chief Information Officer **Response:** [[Add additional relevant information as required.]]
CA-3	**System Interconnections** **Control:** The organization: • Authorizes connections from the information system to other information systems through the use of interconnection Security Agreements; • Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and • Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]. **Response:** [[Add additional relevant information as required.]]
CM-3	**Configuration Change Control** **Control:** The organization: • Determines the types of changes to the information system that are configuration-controlled; • Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; • Documents configuration change decisions associated with the information system; • Implements approved configuration-controlled changes to the information system; • Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; • Andils and reviews activities associated with configuration-controlled changes to the information system; and • Coordinates and provides oversight for configuration change control activities through the: organization-defined configuration change control that convenes organization-defined configuration change conditions. **Response:** • System configuration settings and changes are managed using the University systems Change Management processes and Change Advisory Board (CAB). [[Add additional relevant information as required.]]

ID	SECURITY CONTROLS

CM-8	**Information System Component Inventory**
	
	Control:
	
	• Develops and documents an inventory of information system components that:
	  • Accurately reflects the current information system;
	  • Includes all components within the authorization boundary of the information system;
	  • Is at the level of granularity deemed necessary for tracking and reporting; and
	  • Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
	• Reviews and updates the information system component inventory.
	
	Response:
	
	[[Add additional relevant information as required.]]

CM-10	**Software Usage Restrictions** **Control:** The organization: • Uses software and associated documentation in accordance with contract agreements and copyright laws; • Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and • Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distr bution, display, performance, or reproduction of copyrighted work. **Response:** [[Add additional relevant information as required.]]
CP-2	**Contingency Plan** **Control:** The organization develops a contingency plan for the information system. **Response:** [[Add additional relevant information as required.]]
CP-9	**Information System Backup** **Control:** Conducts backups of user-level information contained in the information system. Conducts backups of system-level information contained in the information system. Conducts backups of information system documentation including security-related documentation; and Protects the confidentiality, integrity, and availability of backup information at storage locations. **Response:** [[Add additional relevant information as required.]]
IA-2	**Identification and Authentication (organizational Users)** **Control:** • The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

ID	SECURITY CONTROLS
	Response: • See SC-8 [[Add additional relevant information as required.]]
IA-8	**Identification and Authentication (non-organizational users)** **Control:** • The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). **Response:** • See SC-8 [[Add additional relevant information as required.]]
MP-2	**Media Access** **Control:** • The organization restricts access to organization-defined types of digital and/or non-digital media] to personnel or roles. **Response:** [[Add additional relevant information as required.]]
PE-3	**Physical Access Control** **Control:** • Enforces physical access authorizations, controls and audits exist. **Response:** [[Add additional relevant information as required.]]
PL-4	**Rules of Behavior** **Control:** • Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; • Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; • Reviews and updates the rules of behavior; and • Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated **Response:** • See AC-8, CM-10 [[Add additional relevant information as required.]]

FOI2024-017 - 2016

ID	SECURITY CONTROLS
RA-3	**Risk Assessment** **Control:** The organization: • Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; • Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; • Reviews risk assessment results [Assignment: organization-defined frequency]; • Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and • Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. **Response:** • See sections 1.4 and 3.0 of this document. [[Add additional relevant information as required.]]
SC-7	**Boundary Protection** **Control:** • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; • Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. **Response:** [[Add additional relevant information as required.]]
SC-8	**Transmission Confidentially and Integrity** **Control:** • The information system protects the confidentiality and; integrity of transmitted information. **Response:** [[Add additional relevant information as required.]]
SI-8	**SPAM Protection** **Control:** The organization: • Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and • Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures **Response:** [[Add additional relevant information as required.]]
SI-12	**Information Handling and Retention** **Control:**

FOI2024-017 - 2016

ID	SECURITY CONTROLS
	• The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements **Response:** • Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf [[Add additional relevant information as required.]]

FOI2024-017 - 2016