PIA Report
Smart Parking System
NIT2242-Data privacy and Cyber Physical System security

Contents

Student Contribution Table

Student Name	Student ID	Part Completed	Contribution Summary

Drishya Pradhan		Part 1- Introduction Part 2 – Privacy Analysis	helped outline what the project is trying to achieve, who the key parties are (the council, vendors, and payment providers), and why the program is necessary for Brisbane. also contributed to mapping out the information flow, including how license plates and sensor data are collected, processed, and linked to user accounts and payments. focused on analysing the types of personal information being collected and how they connect to privacy risks. I answered the guided questions from the PIA template, making sure to identify elements such as license plates as unique identifiers, payment data as sensitive information, and the risk of re-identification from anonymised datasets. I also highlighted that while the system does not collect health or highly sensitive personal data, it still involves indirect identifiers (like parking history) that could reveal patterns about people.
Khushi Khushi		Part 3 – Risk assessment	I identified and described the main privacy risks connected to the Smart Parking System. I worked on developing clear “risk statements” that explained what could go wrong, why it might happen, and what the impacts would be for both users and the council. I also contributed to rating each risk by its consequence, likelihood, and overall severity, which made it easier to prioritise them. I also added details about residual risk ratings to show how much risk would remain even after controls are applied. This made the assessment more practical because it showed that while most risks can be reduced, not all of them can be completely removed.

Ichchha Bhujel		Part 4 – Risk Treatment Plan	Developed detailed risk treatment actions, documented residual risk ratings, assigned risk owners, set review dates, prepared endorsement section, and finalised document control (title, owner, distribution list, related docs, review date).
			Added notes on review frequency and change-management triggers to ensure risks are re-evaluated when system changes occur.
			Filled in residual consequence, likelihood, and risk ratings. Assigned risk owners and set review dates to ensure ongoing accountability.
			Proposed mitigation strategies for each identified risk, including retention limits, anonymisation schedules, vendor privacy clauses, breach response exercises, monthly control reviews, and transparency reporting.

Introduction

The Smart Parking System is part of the Brisbane Smart Mobility Initiative, aimed at making parking in the city easier and more efficient. Right now, finding a parking spot in busy areas can be frustrating and time-consuming. This system helps solve that problem by using sensors and cameras to monitor parking spaces in real time. A mobile app then shows drivers where spots are available, guides them to the location, and allows them to pay securely without needing cash or tickets.

For the project, we assume that drivers will sign up to the app with basic details such as their email or phone number and car registration. Payments won't be handled directly by the council but through secure third-party providers. The technology itself will be set up and maintained by a specialist vendor, while the council manages the overall program. These assumptions keep the design realistic while still meeting the needs of the city.

The way the system works is straightforward: sensors detect whether a parking space is free, and cameras record license plates as cars enter or leave. This information is sent to the central system, which links it to a parking session. The mobile app shows live updates to users, and payments are processed instantly through the payment provider. Any data kept for enforcement or disputes will only be stored for the minimum required time, after which it will either be deleted or anonymised for planning purposes.

Overall, the Smart Parking System is expected to reduce traffic congestion, cut down emissions, save time for drivers, and make parking enforcement more transparent. It is an important step towards modernising Brisbane's parking management and aligns with the city's larger smart mobility goals.

Part 1 – Program background and details

Program	Smart Parking System		
Organisation	Brisbane Smart Mobility Initiative		
PIA Drafter	Drishya Pradhan	Email	[redacted]
Program Manager	Khushi khushi	Email	[redacted]
Privacy Officer	Ichchha Bhujel	Email	[redacted]
Date Completed	13th September, 2025		

Description of the program and parties

The Smart Parking System is a project under the Brisbane Smart Mobility Initiative to reduce congestion and improve parking efficiency in high-traffic areas. The system uses IoT sensors and cameras (including number plate recognition) to monitor parking spaces and provide real-time updates through a mobile app. Drivers can locate available spaces, navigate to them, and pay securely through the app.

The initiative manages the project, a technology vendor provides infrastructure and maintenance, and an authorised payment processor manages transactions. Expected benefits include reduced congestion, time savings, lower emissions, and transparent enforcement. The project is necessary to modernise parking management in Brisbane.

Scope of this privacy impact assessment

This PIA covers collection, storage, and use of personal information such as license plates, user account details, payment data, and parking session locations. It excludes purely technical functions (e.g., sensor-only detections without identifiers). The PIA applies to the initiative and contracted vendors.

Legal authority

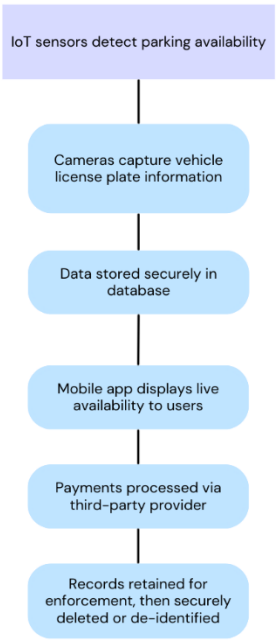
The program aligns with the **Privacy and Data Protection Act 2014 (Victoria)** as a model framework, and relevant Queensland privacy and consumer laws governing data and digital transactions. These laws provide the legal basis for collecting, using, and disclosing personal information.

Stakeholder consultation

Internal stakeholders include program managers, IT staff, and the privacy officer. External stakeholders include technology vendors and community participants consulted through forums. Feedback supported the system provided that privacy protections are strong.

Information flow diagram

1. IoT sensors detect parking availability and send data to the backend.
2. Cameras capture license plates when vehicles enter or exit.
3. Data is stored securely in the initiative's database and linked to parking sessions.
4. The mobile app displays live availability to users.
5. Payments are processed securely via third-party providers.
6. Records are retained for enforcement/disputes, then securely deleted or anonymised.



Part 2 – Privacy analysis

The part identifies the privacy elements and risks the program. The PIA Guide provides guidance on responding to the questions. The right column indicates the relevant section of the PIA Guide. Some questions may not be relevant or applicable. The response should be noted as N/A where this occurs.

The assessment includes prompts to assist identifying the program's elements and risks. There may exist elements or risks beyond each prompt, and each question should be given a broad interpretation. Identified privacy risks should be listed in Part 3. The PIA Guide contains examples of privacy risks that may arise.

Identify the information elements

	Question	*Response*	*Guide*
1	**Does the program involve personal information?** *List each piece of personal information that is involved in the program.*	Yes. It collects license plate numbers, app login details (email/phone), payment data, and parking session locations.	*PART 2* *Section 6*
2	**Does the program involve other information that has the potential to identify individuals?** *This may include information that does not appear to be personal information at first glance, but which could identify individuals based on the context of the project or how the program uses the information.* *Describe this other information and explain how it could potentially identify individuals within the context of the program.*	Yes. Parking history and patterns may reveal daily routines and indirectly identify users.	*PART 2* *Section 6*

3	**Does the program involve sensitive information (as defined under Schedule 1 of the PDP Act)?** *Describe the type(s) of sensitive information that is involved in the program (if any), and how the collection or use of the sensitive information is authorised either by the PDP Act or other legislation.*	No sensitive data such as religion or ethnicity is collected.	*PART 2* *Section 6* *Section 7*
4	**Does the program involve health information?** *If the answer is yes, please refer to the Health Records Act 2001 or consult with the Health Complaints Commissioner in relation to health information (and where applicable, the Office of the Australian Information Commissioner).*	No health information is collected.	*PART 2* *Section 6*
5	**Does the program involve information that has previously been de-identified?** *Describe the type(s) of de-identified information that is involved in the program (if any), and the potential for re-identification.*	Yes. Aggregated and anonymised data may be used for traffic planning. There is a small risk of re-identification if combined with other datasets.	*PART 2* *Section 6*

Collection of personal information

6	**Is all the personal information collected necessary for the program?** *Explain why all the information collected is necessary for the program.*	Yes. License plates enable enforcement, user details support app access, payment data allows billing, and location data supports functionality.	*PART 2* *Section 7*
Privacy risk: If some personal information is not necessary for the program, consider whether there is a risk of overcollection.			
7	**Does the organisation need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?**	No. Enforcement requires identifying vehicles.	*PART 2* *Section 7*
8	**If individuals can remain anonymous, will the organisation be collecting indirect identifiers, such as demographic information?**	No additional demographics beyond basic contact details are collected.	*PART 2* *Section 6*

Method and notice of collection

9	**How will the personal information be collected?** *Describe the means by which the information will be collected. If personal information is collected via a third party platform, explain whether the platform will also be collecting that information*	Through app registration (user input), sensors/cameras (automatic capture), and payment providers (secure transactions).	*PART 2* *Section 7*

Privacy risk: Consider whether the method of collection is fair and not unreasonably intrusive.			
10	**Is the personal information collected directly from the individual?**	Yes, for app and payment details. Vehicle data is collected automatically.	*PART 2* *Section 7*
11	**Will the individual be notified about the collection of their personal information?** *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.*	Yes. Through the app's privacy policy, consent during registration, and signage in parking zones.	*PART 2* *Section 7*
12	**Will any personal information about the individual be collected indirectly from another source?** *Describe how and from which other sources the personal information will be collected.*	Yes. License plate details are collected by cameras.	*PART 2* *Section 7*
Privacy risk: If personal information is indirectly collected, consider whether there is a risk of the information being inaccurate, out of date or incomplete. Consider the impact on individuals if they are not made aware that their information is being collected from another source.			
13	**Will the individual be notified that their personal information has been collected from another source?** *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.*	Yes. Notices and signage will make drivers aware.	*PART 2* *Section 7*

Unique identifiers

14	**Will the program assign a unique identifier or collect a unique identifier assigned by another organisation to adopt as the organisation's own?** *Describe the unique identifier, the purpose for assigning or collecting it, and how this is authorised by either the PDP Act or other legislation.*	No new identifier will be created. License plates act as the unique identifier.	*PART 2* *Section 7*
15	**Does the program require an individual to provide a unique identifier?** *Explain why or how the provision of a unique identifier is necessary for the program.*	Yes. The license plate number is necessary for enforcement.	*PART 2* *Section 7*

Quality of personal information

16	**What steps will the organisation take to ensure the personal information collected is accurate, complete, and up to date?**	System checks, user ability to update details, and periodic audits.	*PART 2* *Section 9*

Privacy risk: If there are inadequate or no steps taken, consider whether there is a risk that the information will be inaccurate, incomplete or out of date.

Security of personal information

17	**Are there security measures in place (existing or intended) to protect the personal information collected and used for this program?** *List the policies, procedures, or controls that the organisation implements to protect personal information. Please indicate how these measures will be governed. Include links or attachments where appropriate*	Yes. Encryption, access controls, activity logging, audits, and staff training.	*PART 2* *Section 8*
18	**Where and how will personal information be stored?** *Describe the format in which the personal information will be stored (e.g. electronic, hard copy etc.) and where it will be stored (e.g. internally, external provider, cloud, third party platform etc.)*	Secure electronic databases or approved cloud services.	*PART 2* *Section 8*
19	**Who will have access to the personal information?** *Describe the positions that will have access how access is gained or controlled, and whether it is logged.*	Only authorised staff with role-based credentials.	*PART 2* *Section 8*
20	**Has a separate security risk assessment been completed?** *If so, please refer to or attach a copy of the assessment to this PIA. If not, OVIC suggests a security risk assessment is completed.*	A security risk assessment will be completed prior to rollout.	*PART 2* *Section 8*

Privacy risk: If there are inadequate or no security measures in place, consider whether there is a risk that the information will not be properly protected, leading to loss, misuse, or unauthorised access, modification or disclosure.

Primary and additional uses and disclosures of personal information

21	**Is the personal information (including any sensitive information) involved in this program used or disclosed for the main or primary purpose for which it was collected?** *Describe what personal information will be used or disclosed, and for what purposes.*	Yes. For parking availability, enforcement, and payments.	*PART 2* *Section 9*

22	**Does the program use or disclose personal information (including sensitive information) for a new or additional purpose other than the original purpose of collection?** *Describe the new/additional purpose for the use or disclosure of the information and explain how it is authorised, by either the PDP Act or other legislation. If relying on IPP 2.1(a), explain how the secondary use or disclosure is related to the primary purpose of collection.*	Yes. Aggregated data may be used for city planning.	*PART 2* *Section 9*

Privacy risk: If relying on IPP 2.1(a) to use personal information for a secondary purpose, consider whether individuals would reasonably expect their information to be used for that secondary purpose. If relying on IPP 2.1(b) to use personal information for a secondary purpose, ensure the individual's consent is meaningful.

23	**Will the individual be notified of the additional use(s) of their personal information?** *Explain how the individual will be given notice of the secondary use(s) of their information, or why notice of the secondary use will not be provided.*	Yes. Through the app's privacy policy and terms of use.	*PART 2* *Section 9*

Transfer and sharing of personal information

24	**Will any personal information be shared outside of the organisation?** *Describe:* • *what information will be shared;* • *with whom the information will be shared;* • *the frequency of the disclosure;* • *how the information will be shared; and* • *how the disclosure is authorised by either the PDP Act or other legislation.* *Identify whether any information sharing agreements are or will be in place.*	Yes. Payment details will be shared securely with licensed processors.	*PART 2* *Section 9*
25	**Will any personal information be transferred outside Victoria?** *Describe what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred. Explain how the transfer is authorised by either the PDP Act or other legislation.*	Possibly, if cloud servers are interstate/overseas, but under contractual safeguards.	*PART 2* *Section 9*

Other considerations relating to use and disclosure

26	**Does the program use or disclose a unique identifier assigned by another organisation?** *Describe the unique identifier and how it will be used or disclosed, and whether this is authorised by either the PDP Act or other legislation.*	No. Only license plates are used.	*Para No. PART 2* *Section 9*
27	**Will any data matching occur as part of this program? This includes matching datasets within the program, or matching to other datasets external to the program.** *If so, explain the purpose for the data matching, what personal information will be matched and what other datasets it will be matched with, and what the combined dataset will be used for.*	Yes. License plates may be checked against enforcement records.	*PART 2* *Section 9*
28	**Will any personal information be de-identified as part of the program?** *Describe the purpose for de-identifying personal information for the program, the method of de-identification, how the de-identified information will be used, and the potential for re-identification.*	Yes. Data will be anonymised for analytics and planning.	*PART 2* *Section 6*
Privacy risk: If personal information is de-identified, consider whether there is a risk that the information can be re-identified. For example, de-identified information may be re-identifiable when matched to other information, or because of the way the de-identified information is used in the context of this program.			
29	**What will be done to ensure the ongoing accuracy, completeness, and currency of the personal information?** *Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.*	Regular system checks, user updates, and monitoring.	*PART 2* *Section 9*

Management of personal information

30	**Is there a document available to the public that sets out the organisation's policies for the management of personal information, such as a privacy policy?** *Identify the document(s) and provide a link where available or include as an attachment to this PIA.*	Yes. A policy will be published.	*PART 2* *Section 10*
31	**Will the document be updated to reflect the new collection or use of personal information for the purposes of this program?** *If not, explain why.*	Yes. The privacy policy will be updated at launch.	*PART 2* *Section 10*

32	**Is there a way for a person to find out the types of personal information the organisation holds about them? Can an individual find out the purposes for which it is held, and how the organisation collects, holds, uses and discloses that information?** *Describe the steps and provide links where relevant.*	Yes. Users can request this information through support channels.	*PART 2* *Section 10*

Access and correction of personal information

33	**How can individuals request access to, or correct their personal information?** *Identify the avenues available for individuals to request access to or correction of their personal information, and who is responsible for handling such requests.*	By contacting customer support or the privacy officer.	*PART 2* *Section 10*

Privacy risk: If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access and correction of personal information held by third parties. If not, there may be a risk that individuals cannot access or correct their personal information.

Retention and disposal of personal information

34	**How long will the personal information be kept for?** *Describe any relevant retention and disposal schedules or policies, including those issued by the Keeper of Public Records or those in other legislation.*	Only for the statutory enforcement period or until disputes are resolved.	*PART 2* *Section 11*
35	**How will personal information be destroyed once it is no longer required?** *Describe the method of destruction and explain how that method is secure.*	Secure deletion protocols will be followed.	*PART 2* *Section 11*
36	**As an alternative to destroying personal information, will any personal information be de-identified once it is no longer required?** *Describe the method of de-identification that will be used and the purposes to which the de-identified information will be put.*	Yes, where possible for long-term planning use.	*PART 2* *Section 11*

Privacy risk: If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.

37	**If applicable, what will happen to personal information held by third parties (such as contracted service providers, cloud storage, third party platforms etc.)?** *Describe any arrangements (for example, any contractual provisions) in relation to third parties' obligations to retain and dispose of personal information.*	Contracts require deletion once data is no longer required.	*PART 2* *Section 11*

Privacy risk: If there are no arrangements in place relating to third parties' retention and disposal of personal information, consider whether there is a risk that personal information will be held indefinitely.

Other considerations

38	**Who can individuals complain to if they have concerns about the handling of their personal information?** *Identify the avenues (internal and external) for making a privacy complaint, including who is responsible for complaint handling.*	Complaints can go to the privacy officer, or escalated to OVIC.	*PART 2* *Section 12*
39	**Does the organisation have a data breach response plan in place?** *If so, describe at a high level the steps that the organisation will take in the event of a data breach.*	Yes. Investigate, contain, notify, and report.	*Para No. PART 2* *Section 12*
40	**Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this program?** *Describe the type of training staff will receive.*	Yes. All staff handling data will complete privacy training.	*PART 2* *Section 12*
41	**Will the program be evaluated against its objectives?** *Describe who will evaluate the program, at what point in the program evaluation will occur, and how often.*	Yes. Regular reviews will check effectiveness and compliance.	*PART 2* *Section 12*
42	**Does the program comply with the organisation's other information handling or information management policies?**	Yes. It aligns with organisational information handling rules.	*PART 2* *Section 12*
43	**Will this PIA be published?**	A summary may be published for transparency.	
44	**Are there any other broader privacy considerations associated with this program?**	Yes. Community trust and clear communication are important.	*PART 2* *Section 12*
45	**Has the organisation's privacy officer been consulted?** *The organisation's privacy officer should be consulted.*	Yes. The privacy officer has been engaged throughout the design process.	

Part 3 – Privacy risk assessment

Were any privacy risks identified in the privacy analysis completed in Part 2 of this PIA?	☒ Yes Enter each privacy risk in the risk assessment table below.	☐ No Proceed to Part 4 of this PIA.

Note: This is a standard risk assessment table. It is recommended that the organisation's own risk assessment framework and table is inserted here. Only use the provided table if the organisation does not have its own risk assessment framework.

	Description of risk	*Consequence rating*	*Likelihood rating*	*Overall risk rating*	*Accept*	*Risk management strategy*	*Residual consequence rating*	*Residual likelihood rating*	*Residual risk rating*	*Owner*
1	**The risk of individual travel routines being identified from continuous parking logs, caused by long-term retention or inappropriate access to location data, resulting in privacy violation, surveillance, and potential misuse of personal movement patterns.**	high	medium	high	no	Keep detailed records only for 90 days, then turn them into grouped, non-personal data that can be used for city planning. Share clear reports so people know how the data is being used	low	low	low	Program Manager – Smart Parking

2	**The risk of personal or payment data breach, caused by a cyber-attack on the app or vendor systems, resulting in the disclosure of card details, license plates, or contact information, leading to financial loss for users and reputational damage for the council.**	high	Medium	high	no	Use a secure and trusted payment system that follows industry standards (PCI-DSS). Store card details in a safe way using tokenisation so the real numbers are not kept. Make sure all data is encrypted when it is sent and stored. Test the system every year to check for weaknesses.	low	low	low	IT Security Lead
3	**The risk of insider misuse of vehicle and location data, caused by staff or contractors accessing records without a valid reason, resulting in unauthorised monitoring and serious breaches of individual privacy.**	medium	medium	medium	no	Apply role-based access, enforce audit logging, conduct quarterly reviews, deliver mandatory privacy training.	low	low	low	Privacy officer
4	**The risk of inaccurate billing, caused by faulty IoT sensors or system glitches, resulting in overcharging or unfair fines for users**	medium	medium	medium	no	Add backup sensors, run data validation, provide a dispute/refund process.	low	low	low	IT Operations Manager

5	**The risk of IoT sensor compromise, caused by weak device security, resulting in attackers injecting false parking availability data and disrupting operations.**	high	medium	medium	no	Apply firmware updates, secure sensor networks, and monitor with intrusion detection.	no	no	no	IT Operations Manage
6	**The risk of security weaknesses, caused by untested code or weak configurations, resulting in successful cyber-attacks that could expose sensitive data and interfere with parking operations.**	high	medium	high	no	Perform full security assessments before rollout, conduct penetration testing, and run mini assessments to catch new weaknesses.	No	no	no	Risk & Compliance Manager
7	**The risk of system-wide compromise, caused by attackers stealing static admin keys, resulting in mass unauthorised access and large-scale data breaches affecting all users.**	high	medium	high	no	Use strong encryption and tokenisation for admin keys, rotate keys every 30 days, and enforce multi-factor authentication for all admin logins.	no	no	no	IT security lead
8	**The risk of delayed breach response, caused by poor incident detection or slow reporting, resulting in greater harm to users and penalties under the Notifiable Data Breaches scheme**	high	medium	high	no	Maintain a detailed incident response plan, rehearse it annually with staff, and notify OAIC and affected users within required timeframes.	no	no	no	Privacy Officer

9	**The risk of re-identification from anonymised data, caused by combining "anonymous" parking records with other datasets, resulting in individuals being identified again.**	medium	medium	medium	no	Apply strong anonymisation techniques, restrict access to aggregated datasets, and perform regular privacy audits.	no	no	no	Data Analytics Lead

**Add more rows by clicking in the bottom right cell and pressing 'tab'

Summary of Risks

Through our privacy risk assessment, we identified a number of risks with the Smart Parking System. Most of these can be managed well through technical measures like encryption, access controls, and regular audits, as well as governance measures such as clear privacy policies and staff training. These steps give us confidence that the majority of risks can be reduced to a low level.

That said, there are a few risks that cannot be fully removed:

1. Travel patterns – Even if we anonymise and delete data after 90 days, it is still possible that some movement patterns could be identified for frequent users. We accept this risk because the overall public benefit (better traffic flow, reduced congestion, easier parking access) outweighs the minimal chance of harm.
2. Vendor risks – Since the system relies on third parties like cloud providers and payment processors, there is always a chance of mishandling outside our direct control. We accept this because outsourcing is necessary for cost efficiency and

expertise, but we will reduce the risk through contracts, audits, and ongoing monitoring.

3. Community concerns – Some members of the public may see the system as surveillance, even if their data is well protected. We accept this as a perception risk, because the benefits (reduced congestion, lower emissions, and convenience for drivers) are significant. To address these concerns, we will use signage, transparency reports, and community engagement sessions to build trust.

We also want to highlight the privacy features that strengthen the program:

- Parking logs are anonymised after 90 days.
- Payments use secure, PCI-DSS certified gateways with tokenisation.
- Staff get privacy and security training.
- Regular reports and audits ensure accountability.

Overall, we believe the benefits of the Smart Parking System outweigh the residual risks, and we have put in place strong safeguards and communication strategies to maintain community trust.

Part 4 – Action items, endorsement, document information

Action items:

The following action items form a comprehensive, risk-based privacy and security implementation plan for the Smart Parking System. For all **high-priority data** — including user passwords, payment identifiers, license plate numbers tied to accounts, and administrative API keys — a **layered protection approach** will be applied, combining **hashing (with salting), tokenization, and encryption** to ensure that even if one control fails, the data remains protected. Administrative API keys and access tokens will additionally be **rotated every 30 days** to minimize the risk of compromise.

Each action item is linked to the specific risk it mitigates, assigned a **priority level** (High, Medium, Low) based on potential impact, and allocated an **owner** to ensure accountability. Timeframes, durations, and end dates are included to make progress measurable, with monthly reviews, log audits, and bi-monthly phishing simulations ensuring that privacy and security controls remain effective over time.

Once actions are completed, owners will update the status and inform the **Program Manager** and **Privacy Officer**. Any delays on **high-priority actions** — particularly those involving encryption, tokenization, anonymization, or key management — will be escalated immediately to the **Executive Sponsor** for review and risk acceptance. This proactive approach keeps the project aligned with privacy laws, security best practices, and evolving threat landscapes, ensuring continuous protection for users and their data.

Action table:

Action	Mitigated Risk	Priority	Owner	End Date	Completed
Apply hash → tokenization → encryption for all high-priority data, including user passwords, payment identifiers, and license plate numbers tied to accounts.	Provides layered protection for sensitive data, ensuring confidentiality even if one layer is compromised.	High	IT Security Lead	15 Nov 2025	☐
Hash, tokenize, and encrypt administrative API keys and access tokens, with 30-day key rotation.	Prevents attackers from using stolen keys to gain full system access, reducing risk of mass breaches.	High	IT Security Lead	18 Nov 2025	☐
Anonymize or securely delete bank account and payment details immediately after each transaction, retaining only non-identifiable metadata (transaction ID, timestamp).	Eliminates stored sensitive payment data, preventing theft in case of breach and reducing fraud risk.	High	Database Administrator / Payment Processor	20 Nov 2025	☐
Implement strong authentication with physical security keys (FIDO2/YubiKey) and role-based access control for staff accounts, with keys re-issued every 6 months.	Prevents phishing attacks, password theft, and unauthorized staff access to sensitive data.	High	IT Security Lead	15 Nov 2025	☐
Conduct monthly access reviews to ensure staff permissions are still appropriate, revoking unnecessary or outdated access.	Prevents privilege creep and insider misuse by ensuring least-privilege is maintained over time.	High	Program Manager / IT Security Lead	First review : 31 Jan 2026	☐
Publish updated privacy policy and install signage in parking areas.	Improves informed consent and reduces user awareness risk.	Medium	Privacy Officer	20 Nov 2025	☐
Provide privacy and security training to all staff handling data, including interactive phishing simulations and social engineering awareness exercises every two months.	Reduces human error, insider misuse risk, and builds a strong security culture through frequent reinforcement.	High	HR / Training Coordinator	30 Nov 2025	☐

Action	Mitigated Risk	Priority	Owner	End Date	Completed
Perform security risk assessment and penetration testing before rollout, and mini assessments every two months post-launch.	Identifies vulnerabilities early and keeps defences updated against evolving threats.	High	Risk & Compliance Manager	25 Nov 2025	☐
Configure data retention schedule and automate secure deletion/anonymisation.	Avoids over-retention, reduces risk of old data exposure.	High	Database Administrator	28 Nov 2025	☐
Draft and sign contractual clauses with vendors for privacy compliance and secure data handling, including clauses requiring vendors to review their security controls monthly.	Mitigates third-party mishandling and legal liability.	High	Legal / Procurement Officer	15 Nov 2025	☐
Establish incident response and data breach notification plan, with tabletop exercises every quarter to keep the team prepared.	Minimizes harm from breaches and ensures compliance with NDB scheme.	High	IT Security Lead	30 Nov 2025	☐
Review privacy controls monthly and update the PIA whenever significant changes or new risks are identified.	Keeps project continuously aligned with privacy best practices and legal requirements.	High	Program Manager	First review: 31 Jan 2026	☐
Audit access logs monthly and investigate anomalies immediately.	Detects unauthorized access and function creep much earlier than quarterly audits.	High	Privacy Officer	First audit: 31 Jan 2026	☐
Engage with community through feedback sessions every six months and publish transparency reports annually.	Maintains public trust and demonstrates accountability.	Medium	Program Manager	First session: 15 Jun 2026	☐
Securely decommission IoT devices and wipe data before disposal, with periodic random checks to verify compliance.	Prevents leakage of stored data from retired equipment.	Medium	IT Operations Team	As required	☐

**Add more rows by clicking in the bottom right cell and pressing 'tab'

Endorsement:

For this project to proceed, all responsible parties listed above — including the CEO, CIO, Executive Sponsor, key stakeholders, and section heads — must review, approve, and provide their signatures. This confirms that they have read and understood the Privacy Impact Assessment, approved the proposed action items, and accepted any residual risks. Only after full endorsement will the Smart Parking System be authorized for implementation.

Name	Position	Signature	Date
Sarah Thompson	**Chief Executive Officer (CEO)**	_____	___ / ___ / 2025
James Patel	**Chief Information Officer (CIO)**	_____	___ / ___ / 2025
Linda Zhao	**Executive Sponsor – Smart Parking Project**	_____	___ / ___ / 2025
Mark Ellis	**Primary Stakeholder Representative – City Mobility Council**	_____	___ / ___ / 2025

**Add more rows by clicking in the bottom right cell and pressing 'tab'

Document information

Field	Details
Document Title	Privacy Impact Assessment – Smart Parking System (Brisbane Smart Mobility Initiative)
Document Location	Brisbane Smart Mobility Initiative – Secure SharePoint (PIA Folder)
Document Owner	Michael Brown – Program Manager, Smart Parking Project
Document Distribution	Sarah Thompson (CEO), James Patel (CIO), Linda Zhao (Executive Sponsor), Mark Ellis (City Mobility Stakeholder), Priya Singh (Privacy Officer), Daniel Reid (IT Security Lead), Rachel Kim (Legal & Compliance Representative), Oliver Grant (IoT Operations

	Lead), **Ichchha Bhujel (Team Member), Drishya (Team Member), Khusi (Team Member)**
Related Documents	Security Risk Assessment Report, Privacy Policy, Data Retention Policy, Incident Response Plan, Vendor Contract Agreements
Next Review	31 January 2026 or sooner if major system changes occur
Document Version	Version 1.0 – Initial Approved PIA (13 September 2025)