Council Dog Infrastructure Model (with login)

Owner: The Council
Reviewer: SENG406 Teaching Team
Contributors: Isla Smyth, Campbell Shephard, Chloe McLaren, Daniel Lowe
Date Generated: Fri Aug 16 2024

Executive Summary

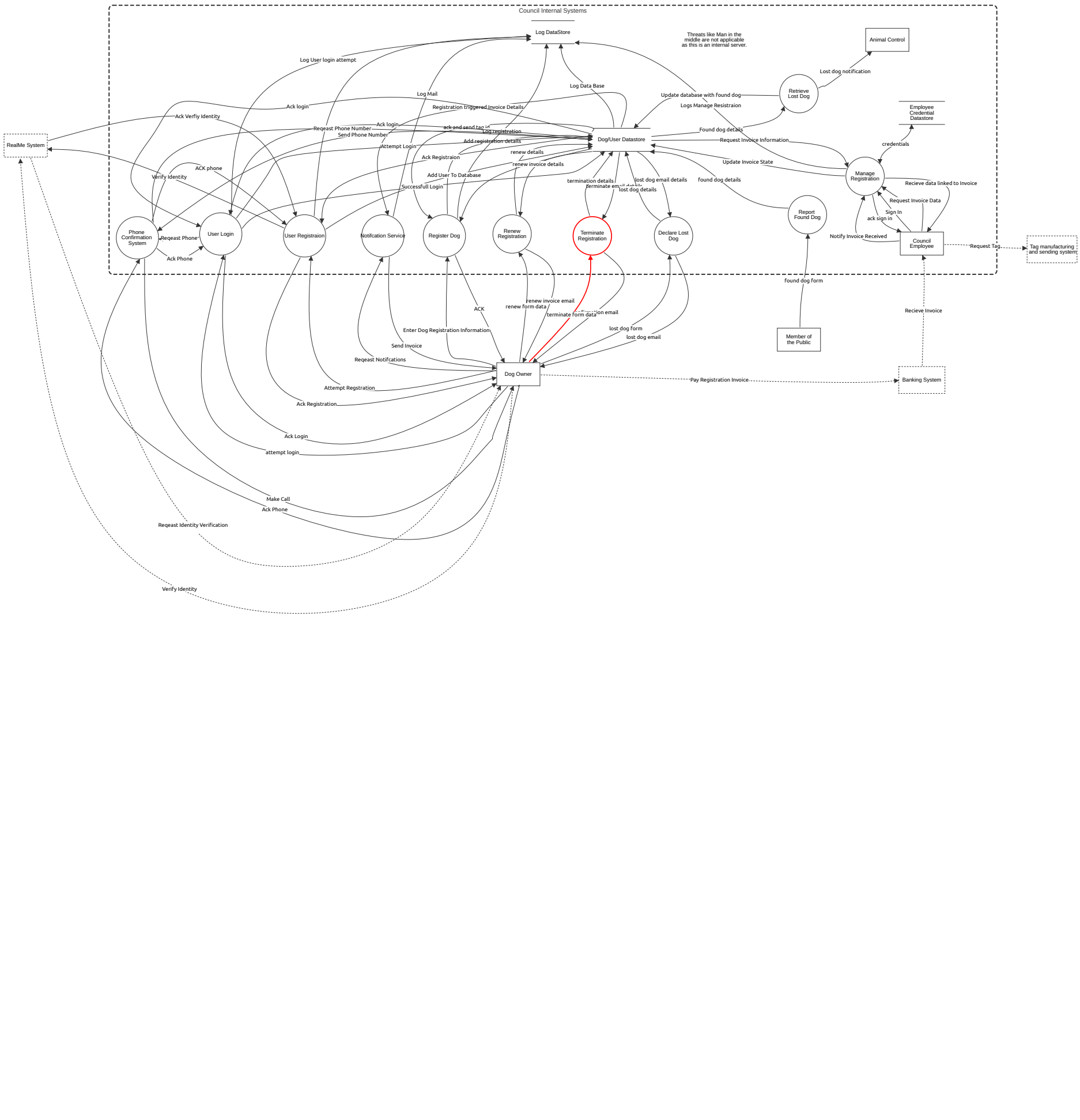
High level system description

Processes that require login do not have dataflows to the datastore and back to represent checking that the user is logged in because it would clutter the diagram well adding minimal information.

Summary

Total Threats	90
Total Mitigated	88
Not Mitigated	2
Open / High Priority	0
Open / Medium Priority	1
Open / Low Priority	1
Open / Unknown Priority	0

Login Diagram



Login Diagram

Dog Owner (Actor)

A person who legally owns one or more dogs and is in the council's range of authority, so wants to register their dog or manage their already existing regulations.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Register Dog (Process)

HTTPS web page endpoint(s) and api(s) that are used for dog registration.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Claim against Registration	Repudiation	Low	Mitigated		Owner performs registration, then claims they didn't register any such dog.	- Log all registration actions to the system. Include relevant information about the request, i.e., IP address, time/date
116	Denial of service	Denial of service	Medium	Mitigated		Someone could flood the end point with fake applications, which causes real applications to be missed as it overwhelms the server.	Rate limit the endpoint Have a white list for allowed requests.

Dog/User Datastore (Store)

Stores information relating to dog and user entities known under the council.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Database Injection	Tampering	High	Mitigated		Injection attacks could be used to change the database's information.	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities - Create frequent backups of the database and store them externally
24	Disclosure by Injection	Information disclosure	Medium	Mitigated		Injection attacks could be used to get information.	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities
25	Flooding Attack	Denial of service	Low	Mitigated		Too many requests in a short amount of time could overwhelm the data store and cause it to stop.	Rate limit interactions with the datastore.
50	Unauthorized Database Access	Information disclosure	Medium	Mitigated		If an attacker gains access to the database, then they could view all the information in the database easily.	Hash all user information by the password with salt so that user information can only be received if you have the user name and password.
117	Repudiation	Repudiation	Medium	Mitigated		Someone could make a change or update to the database and claim that they did not in the future.	Log all requests with the database.

terminate email details (Data Flow)

Contains details for personalising the termination confirmation email that were not obtained in the terminate process: the owner's full name and pronouns, and the registration ID.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

termination details (Data Flow)

Contains tag ID and flag for if a dog's registration has been terminated.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

lost dog email details (Data Flow)

Contains the dog's tag ID, along with details for email personalisation -- owner's full name and pronouns.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Sign In (Data Flow)

Council credentials, including email and password.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ack sign in (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

lost dog details (Data Flow)

Contains the owner's email address, dog's name, and status to update to.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

lost dog email (Data Flow)

Confirmation email for a lost dog declaration, confirming the dog's last known tag ID.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
65	Intercepted email	Information disclosure	Medium	Mitigated		Email could be intercepted and user information could be gained.	Ensure that email is sent over a secure connection using TLS and have checksums.
66	Modified email	Tampering	Medium	Mitigated		Email could be modified to add incorrect information or fake links.	Ensure that email is sent over a secure connection using TLS and have checksums.

lost dog form (Data Flow)

Form consisting of the owner's email address and dog's name.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
63	Flood of fake form requests	Denial of service	Medium	Mitigated		If too many fake form requests are made the servers could get overwhelmed and limit actual users.	Rate limit the number of form requests per user IP. Limit the amount a dog can be lost to once an hour.
64	Man in the middle attack	Tampering	Medium	Mitigated		Form data could be altered with a man in the middle attack allowing for wrong information of dog being lost or for code to be added into the form.	Ensure that HTTPS is used to encrypt the data.

confirmation email (Data Flow)

Personalised email addressed to the owner confirming that the dog of specified ID is no longer registered. Includes a link to the registration page.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	Data Tampering	Tampering	Medium	Mitigated		Data could be tampered with via a man-in-the-middle attack, altering the re-registration link to direct somewhere else.	Ensure the email is sent via TLS.
103	Data Interception	Information disclosure	Medium	Mitigated		The email could be intercepted, allowing an attacker to obtain the owner's pronouns, full name, and email address.	Ensure the email is sent via TLS.

terminate form data (Data Flow)

Form data sent for terminating a dog registration. Contains the owner's email address, tagID, and dog's name.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
99	Data Interception	Information disclosure	Medium	Mitigated		Form data could be intercepted, allowing an attacker to obtain the sender's email address.	Use HTTPS to encrypt the form data.
100	Flooding Attack	Denial of service	Medium	Open		Attackers could flood the termination form page with illegitimate requests, denying its use by legitimate actors.	Rate limit the number of form requests accepted per IP address. Implement a captcha test before forms can be sent. Filter requests upstream using an external protection service, such as Amazon Shield or Cloudflare to check packets against known attacker addresses.

renew invoice email (Data Flow)

Personalised email addressed to the owner, with invoice attached as a PDF.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
92	Interception of Data	Information disclosure	Medium	Mitigated		Email could be intercepted by an attacker, granting them access to the registration owner's pronouns, full name, and email address.	Ensure the email is sent via TLS.
93	Man-in-the-Middle Attack	Tampering	Medium	Mitigated		Data could be tampered with via a man-in-the-middle attack, altering the invoice details, such as amount owed, or the bank account (i.e., if the invoice contains the account number, the number could be altered. If the invoice or email instead contains instructions on where to find the account number, these instructions could be altered, perhaps to point to a spoofed website). The PDF could also be altered to contain malicious executable code.	Ensure the email is sent via TLS.

Request Tag (Data Flow) - *Out of Scope*

The council employee manually requests the tags to be made and shipped to the address that the invoice is related to.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

found dog details (Data Flow)

Contains the dog's tag ID, current status, and possibly the reported sighting address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Found dog details (Data Flow)

Information necessary for animal control to find and return dog.
Last address of dog, dog tag ID, dog breed, owner’s address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request Invoice Information (Data Flow)

The information for the provided reference that is required to send the tag is retrieved, so the dog ID and the address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Update Invoice State (Data Flow)

The invoice is marked as paid for the provided reference.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

credentials (Data Flow)

Employee credentials (i.e., email/password)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Lost dog notification (Data Flow)

Notifies animal control about lost dogs and any information on them.
(Last address of dog, dog tag ID, dog breed, owner’s address, etc)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
75	Information sent to more people	Information disclosure	Medium	Mitigated		Information sent to people in animal control who will not be dealing with the form.	Have the notification only sent to persons who will be collecting the dog

Number	Title	Type	Priority	Status	Score	Description	Mitigations
76	Flooded with fake notifications	Denial of service	Medium	Mitigated		If too many fake notifications are sent then animal control won't be able to accurately collect dogs.	Disallow multiple requests from the same origin IP (IP blocking after multiple calls) within a few seconds. Disallow requests not from known IPs (such as the council) Block IPs from known attackers. Limit the amount a dog can be lost to once an hour.
77	Man in the middle	Tampering	Medium	Mitigated		Man in the middle attack could be performed on the notification if there is an insecure connection, allowing for information sent to animal control to be modified.	Ensure that HTTPS is used to encrypt the data. Verify a dog with the given ID exists and is lost. Verify the last address of the dog is within a reasonable distance of the owner's address. Verify the identity of the owner when returning the dog. Encrypt information.
112	Notification details publicly accessible	Information disclosure	Medium	Mitigated		Malicious actor could intercept information such as dog details, dog location, owner’s address, etc.	Use a secure transfer protocol. Encrypt information.

ack and send tag id (Data Flow)

acknowledges that a regulation was successful and gets the generated unique dog ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Add registration details (Data Flow)

Contains all of the details from the registration form: the human pronoun, first and last name, email address, and physical address, and the dog's name and breed. This information is used to create a new entry in the database.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Logs Manage Resistraion (Data Flow)

Contains all actions taken while managing the registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log Data Base (Data Flow)

Logs every request to the database

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log registration (Data Flow)

Logs all registrations or attempts at registration

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log Mail (Data Flow)

Logs all requests to send mail and all mail that is sent

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Registration triggered Invoice Details (Data Flow)

Once registration details have been updated, invoice details are generated in the database and sent to the mail service.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Pay Registration Invoice (Data Flow) *- Out of Scope*

The dog owner pays for the invoice from their registration with the details listed in the invoice.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Recieve Invoice (Data Flow) *- Out of Scope*

Council employees check that the bank transfers made to the assacated bank account.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Recieve data linked to Invoice (Data Flow)

The employee receives the data linked to the reqeasted invoice so that they can create and send a tag, so the address and the dog id

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request Invoice Data (Data Flow)

The employee enters the invoice reference to find information about the linked dog owner so that they can create and send the tag.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Notify Invoice Received (Data Flow)

The employee notifies the system that they have sent the tag and that the invoice is now paid by providing the invoice refrance.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log User login attempt (Data Flow)

logs a users attempt at logging in

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Update database with found dog (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack Phone (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ACK phone (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack login (Data Flow)

Ack if the login was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

renew form data (Data Flow)

Form consisting of dog's tag ID and new delivery address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
83	Data Tampering	Tampering	Medium	Mitigated		A man-in-the-middle attacker could tamper with the form data, altering the physical address field to send it to.	Use HTTPS to encrypt the form data, and send the form data with a generated hash to ensure it hasn't been tampered.
84	Data interception	Tampering	Low	Mitigated		An attacker could intercept the data sent, obtaining the sender's physical address and tag ID.	Use HTTPS to encrypt the data.

found dog form (Data Flow)

Contains: last address of dog, dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	Insecure connection/Adversary in the middle	Tampering	Medium	Mitigated		An adversary-in-the-middle intercepts the form and modifies its content. (Change location or dog tag ID)	Use Transport Layer Security for the communication Use secure connection, https-only and secure cookie with unique session id. Add encryption/checksums to information.
110	Address publicly accessible	Information disclosure	Medium	Mitigated		When submitting a form, the current location of the member of the public or the dog could be visible to anyone.	Use a secure transfer protocol. Encrypt information.
111	Flooding of forms	Denial of service	Medium	Mitigated		More than one found dog form coming from the same user within a few seconds.	Disallow multiple requests from the same origin IP (IP blocking after multiple calls) within a few seconds. Block IPs from known attackers. Implement Captcha system.

Reqeast Identity Verification (Data Flow) - *Out of Scope*

Reqeast a user identify their identity.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verify Identity (Data Flow) - *Out of Scope*

the User Verifys Identity

Number	Title	Type	Priority	Status	Score	Description	Mitigations

attempt login (Data Flow)

Sends username and password to attempt to login

Number	Title	Type	Priority	Status	Score	Description	Mitigations
121	Man in the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack and manipulate the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.
122	Man in the middle, spying	Denial of service	Medium	Mitigated		Someone could spy on the information while it is in transit.	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.

Ack Login (Data Flow)

Send data that acknowledges the login was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
123	Man in the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.
124	Man in the middle, spying	Information disclosure	Medium	Mitigated		Someone could spy on the information while it is in transit.	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.

Ack Phone (Data Flow)

Sends infomation that the user pressed the # sysmbol and confirmed the login

Number	Title	Type	Priority	Status	Score	Description	Mitigations
133	Man in the middle Tampering	Tampering	Low	Mitigated		Someone could do a man-in-the middle attack and manipulate the data while it is in transit.	Use secure protocols to encypt the data in transit.
134	Man in the middle, spying	Information disclosure	Medium	Mitigated		Someone could do a man-in-the middle attack and view the data while it is in transit.	Use secure protocols to encypt the data in transit.

Make Call (Data Flow)

The phone call that is make to the person

Number	Title	Type	Priority	Status	Score	Description	Mitigations
131	Man in the middle Tampering	Tampering	Low	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	Use secure protocols to encypt the data in transit.
132	Man in the middle, spying	Information disclosure	Low	Mitigated		Someone could do a man-in-the middle attack and view the data while it is in transit.	Use secure protocols to encypt the data in transit.

Ack Verfiy Identity (Data Flow)

Ack knowlages if the person is who they say they are

Number	Title	Type	Priority	Status	Score	Description	Mitigations
147	man-in-the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack and manipulate the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.
148	man-in-the middle Spying	Information disclosure	Medium	Mitigated		Someone could do a man-in-the middle attack and Spy on the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.

Verify Identity (Data Flow)

Uses the real me service to request the user to verify their identity.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
145	man-in-the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack and manipulate the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.
146	man-in-the middle spying	Information disclosure	Medium	Mitigated		Someone could do a man-in-the middle attack and Spy on the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.

ACK (Data Flow)

acknowledges that the registration was successful, and informs the owner of the registration number and expiry date for the registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Spying	Information disclosure	Low	Mitigated		some one could spy on the infomation while it is in transit.	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.
56	Tampering	Tampering	Medium	Mitigated		Acknowledgement could be tampered with; i.e., changing registration number to another registration. Since this is used in the reference for a bank transfer, the owner could end up failing to pay their own registration.	Use HTTPS

Attempt Regstration (Data Flow)

Contains the users

Number	Title	Type	Priority	Status	Score	Description	Mitigations
140	Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack and manipulate the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.
141	Information Disclosure	Information disclosure	Medium	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.

Ack Registration (Data Flow)

Acknowledges if the registration was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
135	Man in the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	By using HTTPS, this is prevented as the data is encrypted in transit, so they could only do this if they got the data from the connection at the very start.
136	Man in the middle, spying	Information disclosure	Medium	Mitigated		Someone could spy on the information while it is in transit.	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.

Attempt Login (Data Flow)

The users username and password are sent(hashed) and checked agenst the data base to see if there is a match

Number	Title	Type	Priority	Status	Score	Description	Mitigations

renew details (Data Flow)

Contains both the old and new tag IDs, the new physical address, and a new expiry date. Sets the flag is_paid to false.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack Registraion (Data Flow)

Ack if the registration was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Add User To Database (Data Flow)

Adds a user to the database with the given details

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack login (Data Flow)

Sends if the login was successfull or not for the user

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Send Phone Number (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Reqeast Phone (Data Flow)

Require a phone call be sent out to the given user.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Reqeast Phone Number (Data Flow)

Require a phone number for a given user

Number	Title	Type	Priority	Status	Score	Description	Mitigations

renew invoice details (Data Flow)

Contains details pertinent to the renew registration email invoice that were not obtained in the web form process: full name, pronouns, registration number, and email address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Successfull Login (Data Flow)

Tell the system the login was successful (after phone).

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Enter Dog Registration Information (Data Flow)

Enters the information for registering a dog.
the human pronoun, first and last name, email address, and physical address, and the dog's name and breed. This information is used to create a new entry in the database.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Data manipulation	Tampering	High	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	By using HTTPS this is prevented as the data is encrypted in transit so they could only do this if they got the data from the connection at the very start.
9	Information Spying	Information disclosure	Medium	Mitigated		Someone could be a man in the middle and spy on people using the application, therefore getting information like their address and email	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.

Reqeast Notifcations (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Send Invoice (Data Flow)

Notifies the user of the invoice.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
149	Data manipulation	Tampering	High	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	By using HTTPS this is prevented as the data is encrypted in transit so they could only do this if they got the data from the connection at the very start.
150	Informatoin disclosure	Information disclosure	Medium	Mitigated		Someone could be a man in the middle and spy on people using the application, therefore getting information like their address and email	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.

Renew Registration (Process)

HTTPS webpage endpoint(s) for renewing a dog's registration.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
86	Website Spoofing	Spoofing	Medium	Mitigated		Someone could create a fake version of this website, causing people to give their information to the wrong people.	- Prioritise shorter URLs - Purchase and redirect from similar domains
87	False Information	Spoofing	Low	Mitigated		Users could provide incorrect renewal details, such as an invalid address.	Validate addresses syntactically and through a location API.
88	Claim against renewal	Repudiation	Low	Mitigated		Owners could claim they hadn't performed a registration renewal when they had.	- Log all renewal actions to the system. Include relevant information about the request, i.e., IP address, time/date
89	Data Interception	Information disclosure	Medium	Mitigated		See renew form data	
90	Data Tampering	Tampering	Medium	Mitigated		See renew form data	
91	Flooding Attack	Denial of service	Medium	Mitigated		See renew form data	
142	Fake Renew	Tampering	Medium	Mitigated		Renew someone else's dog without their consent or knowledge.	Requires you to be logged in, which requires two-factor authentication.

Terminate Registration (Process)

HTTPS webpage endpoint(s) for terminating a dog's registration.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
94	Website Spoofing	Spoofing	Medium	Mitigated		Someone could create a fake version of this website, causing people to give their information to the wrong people.	- Prioritise shorter URLs - Purchase and redirect from similar domains
95	False Information	Spoofing	Low	Open		Users could provide incorrect termination details, such as an invalid address.	Validate addresses syntactically and through a location API.
96	Claim against termination	Repudiation	Low	Mitigated		Owners could claim they hadn't performed a registration termination when they had.	- Log all termination actions to the system. Include relevant information about the request, i.e., IP address, time/date
97	Data Interception	Information disclosure	Medium	Mitigated		See terminate form data	
98	Flooding Attack	Denial of service	Medium	Mitigated		See terminate form data	

Number	Title	Type	Priority	Status	Score	Description	Mitigations
143	Fake Termnate	Tampering	High	Mitigated		Termnate someone else's dog without their consent or knowledge, forcing them to repay the registration fee for their dog.	It requires you to be logged in, which requires two-factor authentication.

Declare Lost Dog (Process)

HTTPS webpage endpoint(s) for declaring a dog as lost.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
67	Fake dog owner	Spoofing	Medium	Mitigated		Someone else fills a fake form that a dog has been lost.	Have a login system for dog owners.
68	Inserted code	Tampering	Medium	Mitigated		Code could be inserted into the form for the server to run.	Check the form inputs for any code.
69	Claim against reporting lost	Repudiation	Medium	Mitigated		Declares a dog lost and then claims later that they did not.	To log the IP date and time when someone claims a dog lost.
70	Too many requests	Denial of service	Medium	Mitigated		If too many requests are sent then the servers get overwhelmed and not be able to handle more lost dogs.	Rate limit the number of form requests per user IP. Limit the amount a dog can be lost to once an hour.
144	New STRIDE threat	Spoofing	Medium	Mitigated		Declare a dog is lost that is not lost, wasting animal control time.	You need to be logged in to declare your dog lost, and any dogs declared lost in this way are logged so if it is found that they are not lost then they can know who lied.

Report Found Dog (Process)

HTTP webpage endpoint(s) for reporting a dog as found.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
78	Fake information	Spoofing	Medium	Mitigated		Someone gives fake information about a found dog	Check for a real address. Log who makes claims and blacklist multiple fake reports.
79	Inserted code	Tampering	Medium	Mitigated		Code could be inserted into the form for the server to run.	Check the form inputs for any code.
80	Claim against finding dog	Repudiation	Medium	Mitigated		Claims they did not make a report for finding a dog.	To log the IP date and time when someone claims to find a dog lost.

Member of the Public (Actor)

Members of the public can report lost dogs they have found.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Incorrect input	Spoofing	Low	Mitigated		Member of the public inputs incorrect dog tag or address (intentionally or unintentionally)	Use location data from the user's device to determine address. Require a photo of the dog tag. Check if the tag with that id exists. Ignore if the dog tag id is not lost within a reasonable distance of the owner's address. Check address is valid.

Council Employee (Actor)

A person who works for the company in an admin role for the system.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
81	Staff credentials could be stolen or guessed	Spoofing	High	Mitigated		Someone could obtain or guess the credentials of a council employee, gaining access to the system when they shouldn't.	Enforce strong password rules (for length and character types, i.e., special characters). Block the use of common passwords and phrases. Require two-factor authentication for logging in. Periodically enforce changing passwords, and disallow the use of previous passwords. Automatically expire user sessions after a period of inactivity (i.e., 30 minutes), and after a total elapsed period (i.e., 8 hours). Consider funding and distributing to staff members an external password service, and educate about its usage.
82	Staff member modifies a registration and claims otherwise	Repudiation	Medium	Mitigated		A staff member with valid credentials could modify a dog's registration in the data store, then claim they didn't modify it.	Log all database transactions and employee logins to a file. Include the details of any transaction performed, along with other relevant information, such as the user who performed it and the time and date it occurred.

Manage Registration (Process)

Council-only end-point for viewing and manipulating the dog registration datastore directly.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
47	Insider Misuse of Personal Data	Information disclosure	Medium	Mitigated		A concil employee could get the personal information of people in the system for their own use e.g., they could get their X address if they have a dog and know some of their personal information.	To request customer data, they need to use the invoice registration number, and only the address and the tag ID will be returned. All actions by the employee are also recorded so that any malicious activity can be found, such as spamming possible dog tags.
118	Insider Misuse of tag paid system	Tampering	Medium	Mitigated		Someone could falsely claim that someone they know has paid for a tag when they have not.	All actions are logged, and work is checked over by other employees.

Employee Credential Datastore (Store)

Stores all council employee credentials.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Notifcation Service (Process)

Used to notify user of changes invoices.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Denial of Service	Denial of service	Medium	Mitigated		Too many mail requests could be made that cause the system to only send some of them.	Rate limit intraction with the notification sender and keep a stack of all the emails that still need to be sent.
115	Fake Invoice	Spoofing	Medium	Mitigated		An attacker could create a fake invoice in the same style as the real invoices and send them to customers they know are getting dogs and are in the area, so that they can steal money from them.	The invoices are sent using the internal system so they would need access to the system to do this.

Banking System (Actor) - *Out of Scope*

Used to transfer money between accounts so that money can be paid

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Tag manufacturing and sending system (Actor) - *Out of Scope*

The system for creating and sending the tags to dog owners

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Retrieve Lost Dog (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Animal Control (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
73	Fake user	Spoofing	Medium	Mitigated		Another person gains access to a animal controllers account	Implement a multifactor login system Enforce strong password polices
74	False claims	Repudiation	Medium	Mitigated		Claim that a dog has been collected when it has not been. Or claim a dog is still missing when it has been found.	Log when user signs in and out and what they interact with.

Log DataStore (Store)

Stores all logs for the system

Number	Title	Type	Priority	Status	Score	Description	Mitigations
130	Injection Tampering	Tampering	Medium	Mitigated		Injection attacks could be used to change the database's information.	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities - Create frequent backups of the database and store them externally

User Registraion (Process)

Registers someone with the provided name and RealMe account and password.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
137	Flood Endpoint	Denial of service	Low	Mitigated		Someone could flood the endpoint with fake login attempts to force the endpoint down.	Use IP blocking to prevent one address from being repeatedly used.
138	Pretend to be someone else.	Spoofing	Medium	Mitigated		Someone could possibly put in fake information to their registration, so if an investigation is needed for a mistreatment of their dogs while they are not at home, then they can blame someone else.	Use RealMe to verify a person's details and request they verify their phone number by calling it.
139	Phishing Attacks	Spoofing	Medium	Mitigated		Fake registration pages designed to steal personal information, including usernames, passwords, and financial details.	- Prioritise shorter URLs - Purchase and redirect from similar domains

User Login (Process)

Used to log users in

Number	Title	Type	Priority	Status	Score	Description	Mitigations
125	Wbsite spoofing	Spoofing	Low	Mitigated		Someone could create a fake version of this website, causing people to give their information to the wrong people.	- Prioritise shorter URLs - Purchase and redirect from similar domains
126	Fake login	Spoofing	Medium	Mitigated		Someone could log in as someone else.	All passwords are required to be at least 8 characters long and contain a number, letter, and special charter. Use a CAPTCHA to prevent them from automating it. Reqiure two factor authencation of the phone call From M1036 Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. (Use 3 attempts and 10 minites before the next allowed attempt from the IP address or for that specific account.)
127	Flood Endpoint	Denial of service	Medium	Mitigated		Some one could flood the endpoint with fake login attempts to force the end point down.	Use IP blocking to prevent one address from being repetedly used.
128	Flood User acount.	Denial of service	Medium	Mitigated		Someone could repeatly fake attempting to login in to an account to trick the system into makeing that account not useable.	Use a CAPTCHA to prevent them from automating it and block IP addresses that repeatedly attempt to login to the same account.

Phone Confirmation System (Process)

rings someones phone and reqires them to press the # for them to login to there account.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
125	Website Spoofing	Spoofing	Low	Mitigated		Someone could create a fake version of this website, causing people to give their information to the wrong people.	- Prioritise shorter URLs - Purchase and redirect from similar domains
126	Fake login	Spoofing	Medium	Mitigated		Someone could log in as someone else.	All passwords are required to be at least 8 characters long and contain a number, letter, and special charter. Use a CAPTCHA to prevent them from automating it. From M1036 Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. (Use 3 attempts and 10 minites before the next allowed attempt from the IP address or for that specific account.)
127	Flood Endpoint	Denial of service	Medium	Mitigated		Some one could flood the endpoint with fake login attempts to force the end point down.	Use IP blocking to prevent one address from being repetedly used.
128	Flood User acount.	Denial of service	Medium	Mitigated		Someone could repeatly fake attempting to login in to an account to trick the system into makeing that account not useable.	Use a CAPTCHA to prevent them from automating it and block IP addresses that repeatedly attempt to login to the same account.

RealMe System (Actor) - *Out of Scope*

The NZ digital ID service.

Number	Title	Type	Priority	Status	Score	Description	Mitigations