Dunwoody_Council_Matrix_PD

System Inventory - GREEN

Q#	Topic (short)	Score	Risk Mitigation	Basis (why it scores this way)
Q1.1	Networks/tenants list	Green	Acceptable	List was provided quickly and completely
Q1.2	Device inventory	Green	Acceptable	List was provided quickly and completely
Q1.3	Use cases (pilot/operational/planned)	Yellow	Inherent	Use cases are listed and categorized; list provided quickly, there are some inherent risks to manage with the nature of the some of the items used - NOTE this is not something th could be reduced based on configuration but is more the nature of what's included
Q1.4	Integrations	Yellow	Inherent	Integrations enumerated; list provided quickly, there are some inherent risks to manage with the nature of some of the integrations listed - NOTE this is not something that could be reduced based on configuration but is more the nature of what's included

Retention and Deletion - YELLOW

Q#	Topic (short)	Score	Risk Mitigation	Basis (why it scores this way)
Q2.1	Retention settings + exceptions	Yellow	no evidence	30 days is stated, but PD indicates retention is set/facilitated by Flock and City staff cannot see and/or manage this setting - recommend Flock look into future plans and potentially allow City admins to see and/or manage this setting
Q2.2	Who can change retention + approvals	Yellow	no evidence	Change control is effectively vendor-mediated; however, City Staff has no visual confirmation on this setting and no control of this setting, therefore, no way to confirm it is set at 30 days and/or remains at 30 days beyond word of mouth
Q2.3	Preservation / legal hold	Yellow	no evidence	No legal hold setting in system; workaround is manual download into case files/evidence.com this does meet the need but there is potential for user-error, high operational/lega risk, recommend Flock look into adding an automated process for legal hold

Access Control, Users, MFA, roles, and lifecycle controls - GREEN

Q#	Topic (short)	Score	Risk Mitigation	Basis (why it scores this way)
Q3.1	Current user list export	Green	Acceptable	List was provided quickly and completely
Q3.2	Non-PD direct logins	Yellow	Policy Requested - PD Agreed	User list/rights/last log in for non-PD was provided quickly, there are some inherent risks to manage with external non-PD users having log in but the export does provide necessa insight - PD should considerconducting periodic access review audits
Q3.3	MFA posture	Yellow	Risk - Flock	MFA enforcement enabled, but is described as optional which means it could be turned off; Flock should consider making this required due to the nature of data i.e. external use MFA requirements
Q3.4	Account lifecycle + access reviews	Yellow	Policy Requested - PD Agreed	Onboarding/offboarding workflow described, SOP included; policy change requested to increase/include users with access in the audits - advised practice but not policy

Sharing governance and external agency access - GREEN

Q#	Topic (short)	Score	Risk Mitigation	Basis (why it scores this way)
Q4.1	External agencies with access	Yellow	Inherent	External agency information is complete and list provided quickly, there are some inherent risks to manage with the nature ofdata sharing - NOTE this is not something that could be reduced based on configuration but is more the nature of what's included
Q4.2	Standing/self-service access	Yellow	Inherent	Confirms external agencies have self-service access; even with auditability, this is a higher-risk governance model, access is to LPR data only with exception of 2 neighboring cities with live, regular audits are conducted but difficult to confirm "reason" for search - LE Officers w/CJIS clearance accessing
Q4.3	Nationwide/broad lookup enabled	Yellow	Risk - Flock	Nationwide lookup participation confirmed; requires enhanced oversight, approvals, and audit routines; however, this is the purpose of the product, Flock could update with "rea time" AI determining potential misuse
Q4.4	Review cadence + removals	Yellow	Policy Requested - PD Agreed	request PD to add to the policy cadence and process for executing and documenting removals/restrictions for external agency access issues
Q4.5	External agency searches visible to Dunwoody	Yellow	Policy Requested - PD Agreed	Yes, export reviewed and includes all information expected, PD should ensure this is included in a policy as listed in Q4.4 - NOTE this is not something that could be reduced based on configuration but is more the nature of what's included

Audit Logs, reason codes, and supervisory oversight -YELLOW

Q#	Topic (short)	Score	Risk Mitigation	Basis (why it scores this way)
Q5.1	Audit log sample (minimum fields)	Amber	Training, Policy, Audits	Several of the searches do not list a reason that is explanatory and with no case number the data is insufficient, recommend additional training and audits to ensure users understand the importance of supplying a good "reason", especially when the case number is not yet available, could also consider adding an event # from CAD to fulfill this criteria, PD should conduct additional training and amend SOP to ensure reason is adequate and reviewed as part of the audit
Q5.2	What PD reviews + cadence + escalation	Amber	Policy Requested - PD Agreed	Annual organizational audit with escalation/discipline described; does meet minimum requirement but cadence is light for this type of review, recommend increasing the frequency to quarterly at minimum, of monthly ideal, and should include multiple reviewers
Q5.3	Misuse detection/investigation documentation	Yellow	Risk - Flock	Describes randomized sampling + chain-of-command escalation; recommend flock incorporate automated process to identify potential misuse "real time"
Q5.4	Case number / reason code requirement	Amber	Training, Policy, Audits	Several of the searches do not list a reason that is explanatory and with no case number the data is insufficient, recommend additional training and audits to ensure users understand the importance of supplying a good "reason", especially when the case number is not yet available, could also consider adding an event # from CAD to fulfill this criteria, PD should conduct additional training and amend SOP to ensure reason is adequate and reviewed as part of the audit

Operational continuity/resilience - GREEN

Q#	Topic (short)	Score	Risk Mitigation	Basis (why it scores this way)

Q6.1	Local storage vs cloud-only + outage procedure	Yellow	Acceptable	Speaking with Flock and PD, confirmed that the cameras have redundancy built in, the backend system does as well but is relying on a single provider; the cloud provider is large and does have built in redundancy but anytime there is a single provider, there is risk; Flock agreed to consider adding additional provider
Q6.2	Escalation path / runbook	Green	Acceptable	Escalation to Flock support/CSM stated
Q6.3	Vendor security incident notification	Green	Acceptable	Specific notification time/date provided (12/23/2025 12:34pm) along with email and link to verify information provided
Q6.3	Contract/SLA breach notification timeframe	Amber	Updated in Contract Proposal	PD unable to confirm SLA breach notification/timeframe; Flock unable to confirm what is a breach and their SLA - need to confirm with legal what is in the contract
Policy, Council transparency artifacts, and public FAQs - GREEN				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q7.1	PD policies/SOPs	Yellow	Policy Requested - PD Agreed	Policy exists for internal misuse, but not external misuse; need to update policy to include as per Q4.4
Q7.2	Governance requirements (PD input)	Yellow	Policy Requested - PD Agreed	Operational justification provided;external sharing is in place but a policy does need to be incorporated for handling misuse
Q7.3	Top 10 public/Council questions (FAQ)	Green	Acceptable	Submitted and answered, adding to presentation
Dunwoody_Council_Matrix_Flock				
SOC2 scope, coverage, and AWS carve-out - YELLOW				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q1.1	Current SOC 2 Type II + scope	Yellow	Updated/inclusive SOC2	Requested SOC2 PDFs/coverage period/scope statement; provided SOC2 is type II recently expired but sufficient, explained cloud vendor has separate SOC2 but not provided
Q1.2	AWS services/regions + carve-out vs inclusive	Yellow	no evidence	Regions are described; carve-out explained but documentation not provided
Q1.3	Shared responsibility matrix	Green	Acceptable	Not provided; referenced trust center and advised would be a 40 page document, not provided; not significant time to read all the reports in the portal to gather the necessary information - updates provided with matrix
Data lifecycle, transmission, encryption, and ownership - GREEN				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q2.1	Data storage/processing + data flow	Yellow	Risk - Flock	High-level description provided, inherent risk in relying on a single provider for even backups
Q2.2	Encryption at rest + key mgmt	Green	Acceptable	Described followed up with further
Q2.3	Encryption in transit	Yellow	Acceptable	Described; transitioning away from deprecated
Q2.4	Device-to-cloud/cloud-to-client protections	Yellow	Acceptable	TLS stated; minimal design data provided
Q2.5	Contract language: City ownership + secondary use limits	Green	Updated in Contract Proposal	handled in new contract proposed language
Access Control, remote access, MFA, PAM, sessions, credentials, and admin access - GREEN				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q3.1	Vendor remote access controls	Green	no evidence	Described at a high level (RBAC, approvals, logging, monitoring) without workflow or any details fulfilling the request
Q3.2	MFA enforcement	Green	no evidence	MFA stated as enforced; exceptions/tenant proof not shown here.
Q3.3	PAM (JIT, vaulting, break-glass, recording)	Green	no evidence	Implements PAM controls without specifics/evidence provided
Q3.4	Provisioning/deprovisioning + RBAC + SoD	Green	no evidence	Describe; also states customers are responsible for tenant lifecycle (reviewed in PD responses) but does not mention any audits; updates provided confirmed audits but unk cadence
Q3.5	Credential storage/password policy/session security	Green	no evidence	Provides minimums/lockout; evidence not shown.
Q3.6	No backdoor accounts	Green	no evidence	Clear assertion; requested written attestation by security leadership as evidence - not specifically provided as requested
Sharing model, oversight controls, and auditablility - YELLOW				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q4.1	Sharing model (standing access vs approvals)	Yellow	Acceptable	Explicitly confirms self-service access for external agencies; high-risk model requiring strong audit exports and governance - audits submitted by PD sufficient for evidence
Q4.2	Granular sharing restrictions	Green	Acceptable	Response is generic and not clearly mapped to product-admin controls (device/network/time/export restrictions) - followup interview clarified
Q4.3	Audit log schema + exportability + external agency activity	Green	Acceptable	Gives limited field list and says logs are viewable in Insights; confirm with Flock if they perform audits to verify sharing is working as intended between external agencies or if it's s it and forget it style - confirmed audits in form of testing new rollouts to confirm working as intended
Q4.4	Reason-for-search/case number enforceable	Yellow	Risk - Flock	States reason required but still relying on person submitting reason code to be specific enough for verification - could include automation to look for "real-time" potential misuse "themes" but minimum is requirement is met
Q4.5	Controls against credential sharing	Green	no evidence	Primarily policy-based but does mention anomaly detection/alerting/enforcement - no evidence provided
Q4.6	Audit log field reductions since 10/1/2025	Green	no evidence	States none; could still provide release notes for evidence
Data deletion, termination/exit, backups, and recovery - YELLOW				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q5.1	Offboarding/termination export/deletion confirmation	Green	Acceptable	Response includes workforce termination controls and general deletion
Q5.2	Deletion permanence + backup retention	Red	Update requested	Provides retention, wiping approach, backup notes; still largely attestation; confirm record retention laws - also, should work to incorporate customer insight into data retention, even if PD can't change the date, they should be able to visibly verify it is set as requested and unchanged
Q5.3	DR/BCP (RPO/RTO + test frequency)	Green	Risk - Flock	RPO 1 hour / RTO 24 hours + annual testing stated; follow good practice; however relying on same provider for backups and production is not ideal practice (even when the provider is big and considered "reliable")
Q5.4	Restore authorization + logging	Green	Acceptable	Describes logging in SIEM and least privilege; does not explain who are "qualified personnel", should at least identify by position/title - clarification provided

Q5.5	Resilience if cloud access is down (device buffering)	Green	Acceptable	Response focuses on cloud vendor failover but still relies entirely on the single vendor, should not rely on single provider
Third Parties, subprocessors, tenancy, and disclosures to government - GREEN				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q6.1	Subprocessor list (purpose/access/monitoring)	Yellow	no evidence	Described; purpose/type-of-access/controls not provided.
Q6.2	Data residency (US-only)	Green	Acceptable	Clear No for outside US; needs contract-suitable statement but directionally meets and/or evidence to show configured to stay inside United States - updates to contract to confirm this is required
Q6.3	Tenancy/isolation controls	Green	no evidence	Multi-tenant + logical isolation described; evidence not provided (tenancy security statement would be sufficient)
Q6.4	Government/legal requests + customer notice	Green	Updated in Contract Proposal	General compliance statement; what is Flock's policy regarding data use and disclosure as mentioned in response, how/is customer notified of requests for data - updates proposed for contract
Security operations, vulnerability management, patching, DDoS, and physical security - YELLOW				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q7.1	Preventive security controls	Green	no evidence	Described; evidence not included
Q7.2	Vulnerability scanning + remediation SLAs	Green	no evidence	SLAs stated (15/30 days); what does Flock consider a security incident as described in the response
Q7.3	Pen test exec summary + remediation status	Green	no evidence	Reports available in portal, what is the frequency of the pen tests by policy; not significant time to read all the reports in the portal to gather the necessary information
Q7.4	Patch/update cadence + firmware authenticity	Green	no evidence	Timelines stated; evidence not included
Q7.5	DDoS mitigation + SLA	Green	no evidence	Control description but evidence not included
Q7.6	Physical security	Green	Acceptable	cloud provider physical security controls are established and considered sufficient for this request
Incident response, breach history, monitoring, and customer communications - AMBER				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q8.1	Breach/security incident history	Red	Risk - Flock	Advised no breach history in last 3 years; however, camera breaches have been highly publicized and should have been mentioned at a minimum (December 2025) - what does Flock consider a breach - updates to contract language to identify
Q8.2	Monitoring stack + anomalous search detection	Green	no evidence	General statement; no tooling list, thresholds, or sample alerts as evidence.
Q8.3	Customer notification commitments	Amber	Updated in Contract Proposal	72-hour statement provided; would like to see what Flock considers a Breach and any documentation/contract showing this requirement - updates proposed in contract
CJIS alignment & Georgia law-enforcement governance - YELLOW				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q9.1	CJIS mapping/boundary	Yellow	no evidence	refered to CJIS document in portal - not significant time to read all the reports in the portal to gather the necessary information
Q9.2	Feature gating/misuse controls	Yellow	no evidence	refered to CJIS document in portal - not significant time to read all the reports in the portal to gather the necessary information
Business continuity, insurance, and accountability - YELLOW				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q10.1	DR/BCP existence + last test	Yellow	no evidence	stated plan exists and is updated with RPO/RTO information provided but no supporting evidence
Q10.2	Cyber liability insurance + COI	Green	Acceptable	States insurance exists but points to Trust Center; COI/limits not included in response; not significant time to read all the reports in the portal to gather the necessary information showed evidence
Q10.3	Security accountability/org	Green	Acceptable	Provides CISO/Privacy Officer + team structure
Q10.4	Security training program	Green	no evidence	Cadence/tooling stated; no evidence provided
Q10.5	Threat intelligence process	Green	no evidence	High-level CTI description; evidence not shown.
City operational integrations (notifications/email) - YELLOW				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q11.1	SMTP integration security	Green	no evidence	High-level description provided, no evidence provided
Q11.2	Role accounts for notifications	Amber	not enough info	unclear response on which accounts are sending notifications from Flock
Contractual governance requirements (Councilmember items) + validation of risk signals- GREEN				
Q#	**Topic (short)**	**Score**	**Risk Mitigation**	**Basis (why it scores this way)**
Q12.1	Freeze online T&Cs / order of precedence clause	Amber	Updated in Contract Proposal	proposed updates for MSA
Q12.2	No secondary use / AI training without approval (clause)	Green	Updated in Contract Proposal	Says Customer data is not used to train AI models but does not provide the enforceable clause language and/or any evidence - proposed updates for MSA
Q12.3	Sharing governance/audit commitments	Green	Acceptable	General least-privilege statements; does not speak to auditing to confirm that settings are working as intended - provided addiitonal details
Q12.4	Mandatory enforceable controls (MFA/logs/breach)	Yellow	no evidence	Assertions provided, but proposed clauses/tenant enforceability evidence not provided - requested enforce MFA
Q12.5	Liability expectations	Green	Updated in Contract Proposal	Response indicates liability limitations/warranty disclaimers but no clear statements to feel confident - does contract include any terms/conditions that cover this - proposed updated language