2026

Cybersecurity Governance, Risk Management & Incident Response

NIST CSF 2.0 baseline & year-end testing commitment

SUMMITFLUX LLC

Current program, enterprise-wide scope, and a commitment to complete penetration testing and issue an updated report by 31 December 2026.

Bastionary / Windfield / All SummitFlux-owned or controlled assets

Report date / baseline cutoff	Edition
16 October 2026 (Pacific Time)	Program baseline • Version 1.0
Next report: by 31 December 2026	Report identifier: SF-SEC-2026-01

01 / CYBERSECURITY REPORT

Report administration & guide

Document control	Record
Entity and document owner	SummitFlux LLC • Product Security
Reporting basis	Program baseline as of 16 October 2026 (Pacific Time); completed incident-response exercise documented internally in SF-IRX-2026-01 v1.0; 2026 Supplemental Cybersecurity Report due no later than 31 December 2026; annual reports by 31 December beginning in 2027.
Version and status	Version 1.0 • Program baseline and reporting cycle; publication review remains to be recorded.
Distribution	Main report: suitable for public-release review. Supporting evidence, detailed gaps, and exercise records: internal annex and profile workbook.
Assessment type	Documentary baseline and active reporting cycle. The completed incident-response exercise is summarized here and documented in detail internally; broader operational findings will be consolidated in the 2026 Supplemental Cybersecurity Report.

Contents

Section	Page
02 Executive assessment and commitment	3
03 Company and enterprise-wide scope	4
04 Security accountability and oversight	5
05 Assessment method and evidence standard	6
06–08 NIST CSF Current and Target Profile summaries	7–9
09 Internal testing and asset-wide assurance	10
10 Risk overview and treatment priorities	11
11 Incident-response readiness	12
12 Reporting sequence and recurring publication	13
13 Current position and reporting sequence	14
14 References and source notes	15

Reading convention: current evidence, adopted procedures, planned activities, and completed results are distinct. This edition records the present baseline and active testing program; “not evidenced” is not a finding that a control has failed.

02 / CYBERSECURITY REPORT

Executive assessment & commitment

SummitFlux is operating its security program under NIST CSF 2.0. Work underway includes governance documentation, asset-scope definition, Current and Target Profiles, execution of the adopted internal penetration-testing authorization procedure, and development of incident-response procedures. SummitFlux Internal Penetration Testing will deliver the company-wide testing commitment below. [1–3,5,M1–M3]

This edition updates the program baseline through 16 October 2026. The first 2026 incident-response exercise was completed on 16 October 2026. It combined a facilitated tabletop with limited technical verification on Bastionary using synthetic accounts and teams. Detailed observations, limitations, corrective actions, and technical evidence are retained in internal report SF-IRX-2026-01 v1.0. The 2026 Supplemental Cybersecurity Report, due no later than 31 December 2026, will consolidate completed penetration-testing coverage, exercise results, remediation and retest status, and the security posture demonstrated by reviewed evidence. Prepared procedures and scheduled assessments are not reported as completed tests.

Reporting dimension	Evidence-based conclusion
Security governance	Executive accountability and testing remit are documented. Management has directed the year-end testing and recurring reporting commitment. [5,M3]
Named framework	NIST CSF 2.0 is applied in this assessment. The companion register addresses all 106 Core outcomes. Framework-wide achievement and a CSF Tier are not asserted. [1,3]
Internal testing	Asset-wide penetration testing is committed for completion by 31 December 2026. Actual findings and coverage will be consolidated in the 2026 Supplemental Cybersecurity Report. [M3]
Response testing / outside assessment	The 16 October 2026 incident-response exercise is completed and documented internally in SF-IRX-2026-01 v1.0. This baseline includes a sanitized summary; no independent or outside assessment is claimed.

Reporting cycle and 31 December 2026 commitment

SummitFlux LLC will complete penetration testing across all SummitFlux-owned or controlled assets by 31 December 2026. The first 2026 incident-response exercise was completed on 16 October 2026; corrective actions and follow-up retesting are now part of the active program. No later than 31 December 2026, SummitFlux will issue a 2026 Supplemental Cybersecurity Report incorporating completed penetration-testing coverage, the completed exercise and corrective actions, remediation and retesting, remaining limitations, and unresolved risk. Beginning with 2027, SummitFlux will issue a consolidated cybersecurity report by 31 December each year, with interim updates following material changes, significant assessments, incidents, or significant findings. [M3]

Current baseline / forthcoming results

This report documents the current program baseline and reporting cycle. The completed 16 October 2026 incident-response exercise is documented internally in SF-IRX-2026-01 v1.0 and summarized here; the 2026 Supplemental Cybersecurity Report will consolidate completed testing, exercise follow-up, remediation, retesting, limitations, and residual risk.

03 / CYBERSECURITY REPORT

Company & enterprise-wide scope

SummitFlux LLC is a small, privately held company developing its own products. Management describes approximately three active personnel, including contractors, and two intended initial security-workspace users. The current documentary baseline is product-led; the year-end testing commitment covers all company-owned or controlled assets. [M1,M3]

Asset group / baseline	Security significance and boundary
Bastionary	SummitFlux's authentication and authorization product line. Identity, permissions, sessions, and tenant separation are central assurance concerns. Customer-operated deployments are not automatically within SummitFlux's testing authority. [6,7]
Windfield	SummitFlux's terrain-aware wind-modeling platform. Management identifies planned university, government, and research accounts. Institutional access and data-isolation controls are assessed as future design requirements, not proven deployments. [5,8,M1]
Corporate, cloud & development assets	Company-controlled networks, endpoints, cloud resources, business applications, identities, repositories, release systems, data stores, logs, and backups. Inventory and test coverage will extend beyond the two named products.
Websites & other connected assets	Company websites and any connected product, laboratory, or manufacturing assets identified in the inventory. Asset existence and applicable test methods will be confirmed; no active testing is reported in this edition.

Coverage and authorization boundaries

The commitment is enterprise-wide, not limited to Bastionary or Windfield. The asset register will include all SummitFlux-owned or controlled assets. For each cybersecurity-relevant asset, testing will be appropriate to its technology, exposure, data, and operational constraints, with coverage traceable to a test record. [M3]

Physical assets without a testable cybersecurity surface will be recorded with a non-applicability rationale rather than counted as penetration-tested. Third-party infrastructure and customer-operated environments are not authorized by this commitment; provider-hosted testing remains within SummitFlux's control and applicable permission boundaries.

Inventory and coverage reconciliation

Record asset owners, environments, data flows, external dependencies, approved methods, test dates, and results. Reconcile coverage before the year-end report; disclose any untested asset, limitation, or shortfall and its corrective action rather than silently excluding it. Planned institutional users do not establish a regulated-data classification.

04 / CYBERSECURITY REPORT

Security accountability & oversight

Executive accountability for SummitFlux's security program rests with James Mulroy, Founder & CEO; Security Lead. The role covers product-security oversight, internal-test authorization, risk decisions, and remediation coordination for the scoped software and infrastructure. [5]

Responsibility	Current basis / formalization status
Accountable executive	The security lead is accountable for delivering the year-end testing and reporting commitment, assigning resources, and reviewing coverage and residual risk. [M3]
Testing authority	Effective 15 October 2026, each internal penetration test requires prior written approval from the security lead and, where responsibility is held by someone else, the relevant system owner. Scope, techniques, testers, dates, exclusions, stop conditions, and changes are documented before execution; findings, remediation decisions, and verification results are retained. [M2]
System ownership	Name an owner for each asset and environment. A founder may hold several roles, but delegation and access must be explicit.
Incident coordination	The public security contact is established. Formally designate incident decision authority, backup coverage, external support contacts, and escalation paths.
Contractor responsibilities	Document each participant's scope, permitted access, confidentiality obligations, onboarding, and access removal. A contractor relationship is not proof that these controls operate.

Reporting commitment & oversight

The reporting cycle begins with this October 2026 program baseline. The first 2026 incident-response exercise was completed on 16 October 2026 and is documented internally in SF-IRX-2026-01 v1.0. A 2026 Supplemental Cybersecurity Report will follow no later than 31 December 2026. Beginning in 2027, a consolidated cybersecurity report will be issued by 31 December each year, with interim updates after material changes, significant assessments, incidents, or significant findings. A monthly operating review and quarterly risk review remain recommended oversight cadences; their historical operation is not asserted. [M3]

Risk acceptance and combined roles

The proposed governance model reserves acceptance of significant residual risk and authorization of disruptive testing to the accountable executive. Record the risk, affected assets, compensating measures, rationale, owner, and review date. Where one person approves and performs a test, use a second-person review when available; document the limitation when independent review is unavailable.

NIST alignment: GV.RR, GV.PO, GV.OV and GV.RM. The internal annex contains an adoption-ready charter and decision records. No board committee, independent oversight body, or separately staffed CISO office is implied. [1,2]

05 / CYBERSECURITY REPORT

Assessment method & evidence standard

NIST CSF 2.0 organizes cybersecurity outcomes into six Functions: Govern, Identify, Protect, Detect, Respond, and Recover. It is an outcomes-based framework rather than a fixed implementation checklist. This review tailors outcomes to SummitFlux's scope and follows the Current/Target Profile method in NIST SP 1301. [1–3]

Evidence state	Meaning in this report
Publicly documented	The cited page contains the statement. Its publication is observable; underlying operational effectiveness is not established by the page.
Management-described	Information was provided for the assessment or application. Supporting records have not yet been examined.
Draft / proposed	A process, policy, target, or exercise has been prepared for adoption or execution. It is not represented as an existing operating practice.
Not evidenced	Sufficient supporting artifacts were not available in this review. This is an evidence limitation, not a confirmed control failure.
Operationally verified	Reserved for a defined procedure performed on actual scoped systems with dated results. Only the specific session-revocation and selected tenant-boundary checks documented in SF-IRX-2026-01 v1.0 support this state; no framework-wide operational-verification claim is made.

Profile construction

The companion workbook inventories all 106 Core subcategories and retains the Current/Target assessment and evidence register. Its action plan is aligned to the current incident-response exercise, the 31 December 2026 penetration-testing deadline, the 2026 Supplemental Cybersecurity Report, and the annual reporting cycle thereafter. Outcome achievement remains open until applicable evidence is reviewed; the following summaries cover all 22 Categories. [1,3,M3]

Assessment limitations

This baseline now incorporates the completed 16 October incident-response exercise at a sanitized summary level. That exercise included limited production technical verification using synthetic accounts and teams; it does not constitute an independent assessment or a complete asset-wide penetration test. Broader configuration, endpoint, backup-restore, supplier, training, and enterprise-wide test evidence remains incomplete. No numerical compliance percentage, independent assurance opinion, or CSF Tier is assigned. NIST does not certify CSF implementations. [9]

Commitments, targets, and implementation

The 31 December 2026 testing/reporting deadline and recurring reporting direction are management commitments. Other target controls and detailed procedures remain proposals until adopted; no implementation result is implied. [M3]

06 / CYBERSECURITY REPORT

Govern & Identify

Accountability, business context, risk decisions, assets, and improvement processes provide the foundation for the scoped security program.

Category	Current evidence	Target / next step
GV.OC **Organizational Context**	Company-wide testing scope is directed; the full asset, stakeholder, obligation, and dependency registers remain to be validated. [M1,M3]	Validate scope, critical services, stakeholders, obligations, and external dependencies.
GV.RM **Risk Management Strategy**	No approved risk appetite or repeatable risk-review records supplied.	Approve proportionate risk criteria, decision rights, and treatment/exception records.
GV.RR **Roles, Responsibilities, and Authorities**	Security lead publicly named; delegation and resource decisions not reviewed. [5]	Document role assignments, alternate coverage, resources, and contractor responsibilities.
GV.PO **Policy**	Internal penetration-testing authorization procedure adopted effective 15 October 2026. Broader security and incident procedures continue to be documented and exercised. [M2]	Maintain controlled versions of the testing procedure and retain dated authorization, finding, remediation, and retest records for each engagement; continue formalizing other security and incident procedures.
GV.OV **Oversight**	Year-end update and recurring reporting are committed. Completed oversight cycles and results are not yet evidenced. [M3]	Record management reviews, measures, decisions, and follow-up actions.
GV.SC **Cybersecurity Supply Chain Risk Management**	No supplier register, due-diligence files, or agreed responsibility matrix supplied.	Inventory critical providers; assess access, dependencies, incident duties, and exit terms.
ID.AM **Asset Management**	Products are identified; full asset, data, and authorized flow inventories not supplied. [M1]	Inventory all company-owned or controlled assets and map cybersecurity-relevant assets to dated testing coverage.
ID.RA **Risk Assessment**	Public intake and internal-testing remit exist; evaluated findings and treatment records not reviewed. [5]	Record threats, assess exposures, verify disclosures, and track risk treatment.
ID.IM **Improvement**	Updated reporting is committed for 31 December 2026; the incident-response exercise was completed 16 October 2026; retest evidence remains pending. [M3,M4]	Track improvement actions and update plans from real tests, incidents, and reviews.

These are category-level documentary summaries, not pass/fail findings. Detailed outcome identifiers, evidence requests, and priorities are in the companion profile workbook. Source framework: NIST CSWP 29, Appendix A. [1,3]

07 / CYBERSECURITY REPORT

Protect & Detect

The priority is to distinguish publicly described product safeguards from the actual configuration and monitoring of SummitFlux's own operating environment.

Category	Current evidence	Target / next step
PR.AA **Identity Management, Authentication, and Access Control**	Product identity features are described; corporate account/privilege evidence not reviewed. [6,7]	Inventory identities, enforce appropriate authentication, least privilege, and tested revocation.
PR.AT **Awareness and Training**	Personnel training, acknowledgment, or role-competence records not supplied.	Provide role-specific training and retain participation and understanding records.
PR.DS **Data Security**	Product protection features are described; internal data handling and restore results not reviewed. [6]	Classify data; validate protection, retention, key access, and backups through restore checks.
PR.PS **Platform Security**	Product logging/stack features are described; deployment baselines and maintenance records not reviewed. [6]	Record baselines, updates, log generation, software controls, and secure release evidence.
PR.IR **Technology Infrastructure Resilience**	Actual segmentation, physical safeguards, resilience, and capacity evidence not supplied.	Document boundaries, environmental safeguards, recovery dependencies, and capacity thresholds.
DE.CM **Continuous Monitoring**	Product audit and risk features are described; monitored coverage and delivery tests not supplied. [6]	Inventory monitored assets and services; validate safe alert generation and routing.
DE.AE **Adverse Event Analysis**	No triage criteria, event correlation, or analyst decision records supplied.	Define declaration thresholds, correlation, scope estimation, and escalation evidence.

These are category-level documentary summaries, not pass/fail findings. Detailed outcome identifiers, evidence requests, and priorities are in the companion profile workbook. Source framework: NIST CSWP 29, Appendix A. [1,3]

08 / CYBERSECURITY REPORT

Respond & Recover

The proposed response design connects detection, incident decisions, containment, evidence preservation, restoration, and continuous improvement. The 16 October 2026 exercise is documented internally; operational incident handling remains to be evidenced. [4]

Category	Current evidence	Target / next step
RS.MA **Incident Management**	Named security lead exists; incident decisions were exercised on 16 October 2026; an adopted incident plan is not yet supplied. [5,M4]	Assign incident roles and apply documented triage, severity, escalation, and recovery decisions.
RS.AN **Incident Analysis**	No investigation record or evidence-preservation procedure demonstrated.	Capture timestamps, actions, provenance, scope, root cause, and uncertainty.
RS.CO **Incident Response Reporting and Communication**	Public vulnerability-contact channel exists; incident-notification workflows not validated. [5]	Maintain stakeholder contacts, approval paths, applicable duties, and communication records.
RS.MI **Incident Mitigation**	Session revocation was verified for synthetic accounts on 16 October 2026; privileged-credential containment and eradication not tested. [6,M4]	Test approved containment in isolation; document eradication and re-entry prevention.
RC.RP **Incident Recovery Plan Execution**	No approved recovery targets or successful restoration records supplied.	Agree recovery criteria; verify restoration assets, perform restore checks, and approve return to service.
RC.CO **Incident Recovery Communication**	No recovery-update process or stakeholder communication record supplied.	Define who approves recovery notices, recipients, updates, and closure messaging.

These are category-level documentary summaries, not pass/fail findings. Detailed outcome identifiers, evidence requests, and priorities are in the companion profile workbook. Source framework: NIST CSWP 29, Appendix A. [1,3]

09 / CYBERSECURITY REPORT

Internal testing & asset-wide assurance

SummitFlux Internal Penetration Testing

SummitFlux Internal Penetration Testing is active under the authorization procedure adopted effective 15 October 2026 and will complete the enterprise-wide assessment by 31 December 2026. Coverage includes Bastionary, Windfield, other company software, and company-owned or controlled systems identified in the asset register. Testing is underway; completed engagement evidence and consolidated results will be incorporated into the 2026 Supplemental Cybersecurity Report. [5,M2,M3]

Bastionary: identity and authorization assurance

The security overview describes token signing, session revocation, identity risk controls, encryption, and tamper-evident audit records. These are product representations. A scoped assessment should identify the tested build and configuration, exercise permitted and denied actions, and preserve the observed results. [6]

The engagement sequence is authorization, controlled execution, evidence capture, finding review, remediation, and retest. Each record will identify actual dates, assets, tested builds, methods, observations, and limitations. The 2026 Supplemental Cybersecurity Report will consolidate the results available through its cutoff; later remediation will be tracked through subsequent interim or annual updates. [M2,M3]

Windfield: design-stage institutional assurance

Planned institutional accounts require evaluation of role assignment, administrative delegation, tenant boundaries, data handling, and research-output integrity as those capabilities are developed. Existing institutional deployments or regulated datasets are not assumed. [M1]

Proposed assurance case	Required test record
Privilege boundaries	Use synthetic, low-privilege and administrative test identities. Record expected/actual authorization behavior and evidence of denied unauthorized actions.
Tenant separation	Use two isolated synthetic tenants and approved test data. Record object, API, and session boundary checks without accessing unrelated real users' data.
API / session boundaries	Record permitted versus denied API actions and expected session behavior, including revocation where implemented; retain sanitized observations and any deviations.
Vulnerability / patch validation	Document the scoped condition, controlled reproduction, remediation decision, and retest. A proposed test is not a finding or successful exploit.

Before each test, document the scope, methods, participants, dates, exclusions, and stop conditions. The 2026 Supplemental Cybersecurity Report will link coverage to completed test records; confidential technical details will remain in controlled internal evidence. [M2,M3]

Risk overview & treatment priorities

The scenarios below are assessment-derived priorities based on the scoped products and limited evidence available. They are not assertions of existing vulnerabilities or past incidents. “First” denotes evidence and treatment work to address early; no numerical likelihood or residual-risk rating is assigned before validation.

Scenario	Potential business effect	First evidence / treatment
R1 Privileged identity or credential misuse	Unauthorized changes to identities, permissions, releases, or infrastructure.	Account inventory; authentication and secret-handling configuration; isolated revocation test.
R2 Broken authorization or tenant boundary	Unauthorized access to another account’s data or functions; loss of product trust.	Synthetic-tenant tests; authorization review; regression and remediation records.
R3 Dependency or release compromise	Untrusted code or changes entering a shipped product or supporting service.	Dependency inventory; change approvals; build provenance and release-integrity checks.
R4 Monitoring or evidence gap	Late discovery, uncertain incident scope, or inability to reconstruct actions.	Log-source inventory; protected retention; safe alert-routing and investigation exercise.
R5 Recovery failure or data integrity loss	Extended outage, unrecoverable data, or unreliable modeling outputs.	Business impact review; recovery objectives; isolated restoration and integrity verification.
R6 Concentrated authority / contractor access	Delayed decisions, excessive access, or loss of continuity when a key person is unavailable.	Delegation and alternate contacts; access review; recorded onboarding/offboarding and risk acceptance.

Risk-decision standard proposed for adoption

Prioritize confirmed exposures by business impact, plausible exploitation, affected data, dependency criticality, and available evidence. Record the basis for each decision and the uncertainty. Do not interpret the absence of test evidence as a low risk. Risks accepted temporarily should have an accountable owner, compensating measures, an expiry/review date, and a documented reconsideration trigger.

NIST alignment: GV.RM-02/04/06, ID.RA-03/04/05/06/07. This report initiates a risk discussion; management approval and operational evidence are needed to finalize the register. [1,3]

Incident-response readiness

Execution status at the assessment cutoff

SummitFlux completed its first 2026 incident-response exercise on 16 October 2026. The exercise combined a facilitated tabletop with limited technical verification on Bastionary using synthetic accounts and synthetic teams. Detailed findings remain in the internal exercise report; no outside assessment is claimed.

The response design follows NIST SP 800-61 Rev. 3: preparation and governance support Detect, Respond, and Recover, while lessons learned feed improvements across the security program. Publishing a plan alone does not demonstrate successful incident handling. [4]

Decision stage	Proposed operating approach	Evidence to retain
Recognize and declare	Triage reports; distinguish suspicious activity from a confirmed incident; assign severity and lead.	Alert/report, timestamp, scope assumptions, declaration rationale.
Contain and preserve	Authorize proportionate containment; restrict affected access; preserve logs and configuration with provenance.	Approvals, affected identities, action log, evidence index.
Investigate and communicate	Estimate impact and root cause; involve system owners and providers; review notification obligations.	Known/unknown facts, stakeholder decisions, approved notices.
Restore and close	Validate clean recovery assets and restored service; confirm integrity; approve return to service and follow-up.	Recovery criteria, test results, approval, corrective-action owners.

Completed 2026 incident-response exercise

The completed exercise used a suspected privileged-credential compromise and possible cross-tenant-access scenario for Bastionary. It evaluated decision authority, evidence availability, escalation, communications, containment, and recovery authorization. Limited technical verification confirmed selected session-revocation and synthetic tenant-boundary behaviors. Testing used synthetic accounts and teams; detailed findings and corrective actions remain internal.

The exercise is documented in internal report SF-IRX-2026-01 v1.0, dated 16 October 2026. The 2026 Supplemental Cybersecurity Report will summarize the completed exercise separately from penetration-testing results, including the real date, method, findings, limitations, corrective actions, and any verified technical checks. No outside assessment is inferred.

Exercise scope, participants, date, authorization, observations, limitations, and corrective actions are recorded in SF-IRX-2026-01 v1.0. This public baseline records only a sanitized summary; the 2026 Supplemental Cybersecurity Report will incorporate reviewed follow-up and retest status.

Reporting sequence & recurring publication

The current program baseline is documented in this edition and now includes the completed 16 October 2026 incident-response exercise at a sanitized summary level. Management's delivery commitment is to complete asset-wide penetration testing and issue the 2026 Supplemental Cybersecurity Report no later than 31 December 2026. Beginning in 2027, SummitFlux will publish a consolidated annual cybersecurity report by 31 December each year. The work sequence below supports those commitments; individual engagement windows and resources will be set during authorization. [M3]

Stage / deadline	Priority work	Completion evidence
Current phase	Reconcile the company-wide asset inventory; assign owners; finalize engagement scope, methods, permissions, and dates.	Asset register; ownership and applicability records; written test authorizations.
Testing cycle	Execute authorized testing across cybersecurity-relevant assets; review findings, retest fixes, and record the separate incident-response exercise status.	Dated methods and observations; findings; asset coverage; fix/retest records; exercise evidence where completed.
By 31 December 2026	Complete asset-wide penetration testing and issue the 2026 Supplemental Cybersecurity Report describing the resulting security posture.	Coverage reconciliation; completed internal reports; residual-risk and remediation status; reviewed report.
By 31 December annually beginning 2027	Issue a consolidated cybersecurity report by 31 December each year, plus interim updates after material changes, significant assessments, incidents, or significant findings.	Versioned reports with actual cutoffs; updated profiles; new test results and action status.

Evidence for the supplemental and annual reports

Evidence dimension	Record in the results report
Asset-level test coverage	Identified cybersecurity-relevant assets, the tests actually completed, and any remaining coverage gaps; disclose non-applicability separately.
Findings and remediation	Observed issues, impact/severity basis, disposition, fixes implemented, retest results, and outstanding actions.
Incident-response exercise	Actual exercise date, participants, method, observations, limitations, corrective actions, and technical verification, if performed; keep tabletop decisions distinct from technical results.
Current / Target Profile	Changes supported by reviewed evidence, residual risks, and the next assessment priorities; no unverified compliance score.

The internal incident-response exercise report, SF-IRX-2026-01 v1.0, records the actual exercise date, participants, method, evidence, observations, limitations, and corrective actions. The 2026 Supplemental Cybersecurity Report will state its actual test dates and evidence cutoff and will incorporate the reviewed exercise summary. Beginning in 2027, annual reports will be issued by 31 December, with interim updates for material changes, significant assessments, incidents, or significant findings. Any incomplete coverage or unresolved remediation will be disclosed; planned activities will not be counted as completed results. [M3]

Current position & reporting sequence

Reporting dimension	Section / supporting record	Current conclusion
Accountable security leadership	Sections 02 and 04; public leadership statement [5]; management scope [M1].	Leadership is documented; the internal testing authorization procedure is adopted and the year-end testing/reporting commitment is recorded. Broader recurring oversight records continue to mature. [M2,M3]
Named cybersecurity framework	Sections 05–08; NIST references [1–4]; 106-outcome companion register.	Framework mapping and targets are prepared. Enterprise-wide implementation, effectiveness, and a Tier are not established.
Internal adversarial testing	Sections 03, 09 and 12; internal test records; management commitment [M3].	Internal penetration testing is active under the adopted authorization procedure. Complete asset-wide testing and publish actual coverage, findings, remediation, retests, and limitations by 31 December 2026. [M2,M3]
Incident-response testing or assessment	Section 11; internal exercise report SF-IRX-2026-01 v1.0 [M4].	The 16 October 2026 incident-response exercise is completed and documented internally. This baseline includes a sanitized summary; no outside-assessment evidence is claimed.

Management commitment and report review

Management direction of 15 October 2026 established this reporting sequence: the current baseline; an incident-response exercise report, completed on 16 October 2026; the 2026 Supplemental Cybersecurity Report by 31 December 2026; and annual reports by 31 December beginning in 2027. This does not approve individual engagements or establish completed controls.

Management record	Commitment and publication review
Reviewer	James Mulroy — Founder & CEO; Security Lead
Program commitment	Incident-response exercise completed 16 October 2026; asset-wide testing and 2026 Supplemental Cybersecurity Report by 31 December 2026; annual report by 31 December beginning in 2027. [M3,M4]
Publication review / signature	To be recorded by the authorized reviewer; no signature is applied in this edition.

References & source notes

[1] NIST. The NIST Cybersecurity Framework (CSF) 2.0. CSWP 29, 26 February 2024. Sections 2–3 and Appendix A.

https://doi.org/10.6028/NIST.CSWP.29

[2] NIST. Cybersecurity Framework 2.0: Small Business Quick-Start Guide. SP 1300, February 2024.

https://doi.org/10.6028/NIST.SP.1300

[3] NIST. Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles. SP 1301, February 2024.

https://doi.org/10.6028/NIST.SP.1301

[4] NIST. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. SP 800-61 Rev. 3, April 2025. Sections 2–3.

https://doi.org/10.6028/NIST.SP.800-61r3

[5] SummitFlux LLC. Security at SummitFlux. Page states last updated 16 October 2026; reviewed at the assessment cutoff.

https://summitflux.com/security.html

[6] SummitFlux LLC. Bastionary Security Overview. Public product representations; reviewed at the assessment cutoff.

https://bastionary.com/security.html

[7] SummitFlux LLC. Bastionary product website. Product scope and identity/authorization features; reviewed at the assessment cutoff.

https://bastionary.com/

[8] SummitFlux LLC. Windfield product landing page. Public title identifies terrain-based wind modeling; institutional-account roadmap is management-provided.

https://windfield.summitflux.com/

[9] NIST. Cybersecurity Framework Frequently Asked Questions. Framework scope and certification limitations; reviewed at the assessment cutoff.

https://www.nist.gov/cyberframework/faqs

[M1] Management-provided company and product information, 15 October 2026: approximate active personnel including contractors; intended security-workspace users; company ownership of products; planned Windfield institutional accounts. Unverified management information.

[M2] Management-adopted internal penetration-testing authorization procedure, effective 15 October 2026: each engagement requires prior written approval, defined SummitFlux-owned or controlled scope, permitted techniques, named testers and test accounts, dates, exclusions, stop conditions, renewed approval for scope or timing changes, and documented findings, remediation decisions, and verification results. Operating records are retained per engagement.

[M3] Management direction, 15 October 2026: complete penetration testing across all SummitFlux assets by 31 December 2026; completed incident-response exercise documented in SF-IRX-2026-01 v1.0; issue a 2026 Supplemental Cybersecurity Report no later than 31 December 2026; and issue a consolidated cybersecurity report by 31 December each year beginning in 2027, with interim updates for material changes, significant assessments, incidents, or significant findings. This is a forward-looking commitment except where later evidence documents completed work.

[M4] Completed incident-response exercise, 16 October 2026: SF-IRX-2026-01 v1.0. Facilitated tabletop plus limited technical verification on Bastionary using synthetic accounts and teams. The internal report records actual observations, limitations, corrective actions, and selected technically verified controls. Detailed findings remain confidential; this public report uses a sanitized summary.

Source standard: NIST provides the framework; company pages provide public representations; M1 provides management scope; M2 records the adopted internal testing authorization procedure; M3 records the current management commitment; M4 records the completed incident-response exercise. Recommended implementation details are not NIST-mandated controls.