

PUBLIC SAMPLE / FICTIONAL ENGAGEMENT

Social account security review

Prepared for Northline Studio

A fictional organization used solely to demonstrate reporting. No client information, live indicators or actual evidence is included.

Report reference	Reporting cutoff	Intended reader
SEC-001	07 Oct 2026 / 23:59 UTC	Account owners, marketing operations and IT

EXECUTIVE ASSESSMENT

The fictional Northline Studio has recoverable ownership records, but its administrator lifecycle is inconsistent. Two of eight named administrators lack recorded strong authentication, a former agency retains one elevated role, and one recovery mailbox has no documented backup owner. No compromise is established by this review.

DECISION REQUESTED

Approve the access cleanup and recovery rehearsal before the next campaign launch. Keep emergency access available during changes.

Inside this report

02 Scope and method / 03 Findings / 04 Evidence and chronology / 05 Action plan / 06 Handover and limitations

Illustrative format only. Final scope, response cadence, authorized recipients and local requirements are agreed for each engagement. No service outcome or legal determination is promised.

02 / HALDEN INTELLIGENCE

Scope, coverage & method

AGREED QUESTION AND COVERAGE

Review six business-owned social assets and eight named administrators using owner-supplied role exports, a supervised settings walkthrough and a recovery exercise. Assessment window: 1-7 October 2026. This sample is an assurance snapshot, not continuous monitoring.

OUTSIDE THIS ASSESSMENT

No passwords, session tokens, private messages, penetration testing or direct account administration. Settings were not independently obtained from platform backends.

Asset / record	Accountable owner	Coverage
AS-01 / Business portfolio	Marketing lead	Four internal and two agency roles; ownership attested
AS-02 / Social pages	Channel manager	Three pages; two linked identity accounts
AS-03 / Video channel	Content lead	One channel; delegated access reviewed
AS-04 / Recovery mailbox	IT lead	Business mailbox; backup ownership unresolved

REPORTING METHOD

Define authority and scope; register supplied material; separate direct observations from statements; assess alternative explanations; review findings against source limitations; assign actions with acceptance evidence.

CONFIDENCE IS NOT SEVERITY

High: the cited material directly supports this narrow observation. Moderate: the observation has support but an important gap remains. Low: it is a lead or statement requiring corroboration. Confidence never establishes identity, intent or legal liability.

PRIORITY AND TIME

High: address promptly because of potential material harm or dependency. Medium: assign a near-term owner. Low: review in the agreed cycle. These are qualitative priorities, not CVSS ratings. All times are UTC; event times and receipt times are distinct.

03 / HALDEN INTELLIGENCE

Findings & interpretation

F-01 / HIGH PRIORITY / MODERATE CONFIDENCE

Strong authentication not recorded for two administrators

Observation. Six of eight entries in the supplied register show strong authentication enabled. Two are blank; a blank is not proof that protection is absent.

Why it matters. An unprotected privileged identity could expose several linked assets.

Alternative / uncertainty. The register may be out of date. Confirm through an owner-led settings review before concluding that a control is missing.

Recommended action. Verify the two accounts, enable the strongest supported MFA, and retain only status evidence rather than authentication secrets.

Evidence: E-01, E-02

F-02 / HIGH PRIORITY / HIGH CONFIDENCE

Former agency retains an elevated role

Observation. The role export lists Agency Role B; the engagement roster records its contract as ended. The owner confirms no current business need.

Why it matters. Unnecessary access increases the number of identities able to change the business portfolio.

Alternative / uncertainty. No evidence indicates misuse by the agency. The finding concerns access governance only.

Recommended action. Have the asset owner remove the role after checking ownership dependencies and preserve a before/after record.

Evidence: E-01, E-03

F-03 / MEDIUM PRIORITY / MODERATE CONFIDENCE

Recovery ownership depends on one person

Observation. The exercise could identify the primary mailbox owner but could not establish an approved deputy.

Why it matters. Absence or departure could delay response even when the account is not compromised.

Alternative / uncertainty. A deputy may exist outside the reviewed records; this remains unverified.

Recommended action. Document a deputy, secure recovery materials in the client's controlled vault and rehearse access without exposing codes.

Evidence: E-02, E-03

04 / HALDEN INTELLIGENCE

Evidence & chronology

Evidence register

ID / source	Receipt time (UTC)	Known limitation
E-01 / Fictional role-register export	2026-10-02 09:00 UTC	Point-in-time owner export; completeness unverified
E-02 / Fictional supervised settings notes	2026-10-03 10:00 UTC	No credentials collected; settings may change
E-03 / Fictional roster and recovery exercise	2026-10-05 14:00 UTC	Owner statements corroborate role purpose only

Event chronology

Event time (UTC)	Recorded event	Source
02 Oct / 09:00	Register received and asset owner recorded	E-01
03 Oct / 10:00	Settings walkthrough completed	E-02
05 Oct / 14:00	Agency role and deputy gap confirmed	E-03

HANDLING AND PROVENANCE

The entries above are invented descriptions, not evidence attachments. In a real engagement, assign a unique evidence ID; record collector, authority, source, collection and receipt times, method and limitations; retain the original in approved storage; and log access, transformations and transfers. Calculate digests on actual files where appropriate. Never invent a digest or custody event.

SOURCE BOUNDARIES

A screenshot can support what was visible in that copy. It does not, on its own, prove origin, completeness, authorship or the full history of an event. Preserve contradictions and distinguish client-reported events from independently verified observations.

05 / HALDEN INTELLIGENCE

Action plan & service register

When	Owner	Completion evidence	State
Within 2 business days	IT + asset owner	Verify MFA for two entries; retain status confirmation	Open
Within 2 business days	Marketing owner	Remove obsolete role after dependency check; attach export	Open
Within 7 days	IT lead	Approve deputy and complete recovery rehearsal	Planned
At 30-day review	Case owner	Recheck all eight roles and close evidenced actions	Planned

Control register

Control	Reviewed result	Closure evidence
Ownership	6 of 6 assets have an attested owner	Current signed asset register
MFA status	6 recorded; 2 unverified	Owner-led confirmation for remaining identities
Offboarding	1 obsolete role found	New export showing role removed
Recovery deputy	Not demonstrated	Successful documented rehearsal

Counts describe this fictional sample only. Attested ownership is not a platform determination of ownership.

CLOSING AN ACTION

Record the actual completion time, responsible person and evidence reference. A request, recommendation or platform submission is not completion. Keep unresolved dependencies visible and agree the next review date with the client.

Limitations & handover

LIMITS ON RELIANCE

The review cannot establish that no unauthorized sessions exist. Recheck after administrator, agency, mailbox or platform changes.

DISTRIBUTION AND RETENTION

This fictional sample is public. A live report requires an approved recipient list, secure delivery method, retention schedule and disposal owner agreed with the client and, where relevant, counsel. Do not place real evidence or personal data in public website assets.

Release checklist for a live engagement

Required check	Record to complete before issue
Authority and scope	Approved instruction reference and authorized assets
Analyst and peer review	Named preparer, reviewer, review date and corrections
Client decisions	Decision owner, accepted actions and unresolved objections
Delivery and acceptance	Approved recipients, transfer receipt and acceptance date
Follow-up and retention	Next review, retention basis and disposal responsibility

These fields are deliberately unsigned. No real review, instruction, client approval or evidence transfer is represented by this sample.

Method references

Background guidance only; these publications do not validate fictional findings or certify this report. Apply current platform procedures and engagement-specific legal advice separately.

CISA — Implementing Phishing-Resistant MFA (2022)
<https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>

NIST SP 800-61 Rev. 3 — Incident Response Recommendations and Considerations for Cybersecurity Risk Management (2025)
<https://csrc.nist.gov/pubs/sp/800/61/r3/final>