PUBLIC TRUST & ASSURANCE · PT-FIN-IR-001

Paulioskos Finance Security & HMRC Incident Response Procedure

Defines the public response framework Paulioskos follows for security incidents affecting Finance, HMRC connectivity or personal data, while keeping sensitive operational runbook details restricted.

Version	Effective	Last reviewed	Owner
1.0	13 September 2026	13 September 2026	HR & Compliance Director & Finance Technical Owner

PUBLIC PROCEDURE / RESTRICTED RUNBOOK

This public procedure states the response commitments Paulioskos follows. Private contact numbers, credentials, hostnames, recovery commands, security tooling and evidence locations are maintained separately in a restricted internal runbook so publication does not weaken security.

Documents are reviewed periodically and whenever there is a material change to Finance functionality, controls, suppliers, legal obligations or risk profile.

This controlled procedure explains how Paulioskos Tech Consulting Ltd (“Paulioskos”) identifies, contains, assesses, records and escalates security incidents affecting **Paulioskos Finance**, including incidents involving HMRC Making Tax Digital connectivity or personal data.

It is intentionally public so customers, suppliers, regulators and other third parties can understand the response framework Paulioskos commits to follow.

This document is a governance procedure, not an operational playbook. Sensitive implementation details such as private telephone numbers, credentials, hostnames, recovery commands, security tooling and evidence locations are maintained separately in restricted internal runbooks.

1. Scope

This procedure applies to security events that may affect:

- Paulioskos Finance application services;
- Finance databases and financial records;
- uploaded invoices, receipts and supporting evidence;
- Microsoft Entra authentication or Finance user accounts;
- HMRC OAuth authorisation, access/refresh tokens or application credentials;
- HMRC Making Tax Digital API connectivity;
- production environment configuration, certificates or cryptographic keys;
- Finance backups and recovery copies;
- personal information processed by Finance; or
- the confidentiality, integrity or availability of Finance.

It applies to development, test and production environments, with production and personal-data incidents receiving priority according to risk.

2. Reporting security concerns

Paulioskos provides a public route for customers, suppliers, security researchers and other third parties to report suspected security risks or incidents.

Security concerns may be reported to **security@paulioskos.com**. The Paulioskos Trust Centre and Responsible Vulnerability Disclosure Policy provide the current public reporting route and scope.

Reports should include, where safely possible:

- what was observed;
- the affected service or URL;
- approximate date and time;
- steps to reproduce or supporting evidence;
- whether personal, financial or HMRC-related data may be involved; and
- safe contact details for follow-up.

Reporters should not access, alter, download or retain information beyond what is reasonably necessary to demonstrate the issue.

3. Roles and accountability

HR / Compliance Director

Owns governance, privacy and regulatory coordination, including assessment of notification obligations and maintenance of incident records.

Finance Technical Owner

Leads technical containment, investigation, recovery, credential/token rotation, service restoration and technical evidence preservation.

Directors / authorised management

Provide escalation and business-impact decisions where an incident is material, prolonged, legally significant or requires external notification.

Specific named contacts and telephone numbers required for regulator or HMRC notifications are maintained in the restricted internal incident runbook rather than this public document.

4. Response lifecycle

Paulioskos uses the following response sequence:

1. **Identify and log**

Record the initial report, discovery time, affected systems and known facts.

2. **Triage and classify**

Assess whether the event affects confidentiality, integrity, availability, financial records, personal information, HMRC connectivity or credentials.

3. **Contain**

Take proportionate action to stop or limit further harm.

4. **Preserve evidence**

Retain relevant logs, timestamps, audit records, correlation IDs, affected artefacts and other evidence without unnecessarily exposing secrets or personal information.

5. **Investigate and assess impact**

Determine scope, root cause, affected records/users, likely consequences and whether external notification thresholds are met.

6. **Eradicate and recover**

Remove the cause, patch or reconfigure affected components, rotate/revoke credentials where necessary, restore trusted data/services and validate recovery.

7. **Notify where required**

Notify HMRC, the ICO, affected individuals, customers, suppliers or other authorities where the applicable threshold is met.

8. **Review and improve**

Document lessons learned, corrective actions, ownership and completion dates.

5. Immediate containment actions

Depending on the incident, Paulioskos may:

- suspend or restrict user access;
- terminate active sessions;
- disable affected application functions;
- isolate systems or network paths;
- revoke or rotate Microsoft, HMRC or application credentials;
- revoke HMRC OAuth authorisation or invalidate stored token material;
- rotate encryption keys or certificates where appropriate;
- place Finance into a controlled maintenance state;
- stop outbound email or API activity where it could increase harm;
- preserve a protected recovery point; and
- temporarily block deployment or change activity.

Containment actions are selected according to risk and should avoid unnecessary destruction of evidence.

6. HMRC-related security incidents

A security incident involving HMRC connectivity may include:

- compromise or suspected compromise of HMRC OAuth tokens;
- compromise of an HMRC application client secret;
- unauthorised HMRC API access;
- exposure or manipulation of HMRC-derived data;
- incorrect or falsified fraud-prevention information;
- misuse of a production HMRC application;
- unauthorised VAT submission capability; or
- a breach affecting personal/customer data connected with HMRC API use.

Where an incident concerns the security of personal or customer data and falls within HMRC's reporting requirements, Paulioskos will:

- report the issue to HMRC immediately through the HMRC Developer Hub support/ticket process;
- provide a breach contact name and telephone number through the restricted reporting channel;
- provide full available details to HMRC within 72 hours, updating the ticket as the investigation develops;
- preserve evidence of the notification and subsequent communications; and
- coordinate any related ICO or affected-person notification where legally required.

Paulioskos will not publish HMRC client secrets, OAuth tokens, private support-ticket content or other restricted credentials as part of a public incident notice.

7. Personal data breaches

Every suspected personal data breach is recorded and assessed, whether or not external notification is ultimately required.

Where a personal data breach is notifiable to the Information Commissioner's Office ("ICO"), Paulioskos will notify the ICO **without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach**.

The assessment will consider:

- the nature and sensitivity of the information;
- the number and categories of individuals/records affected;
- whether the information was encrypted or otherwise protected;
- the likelihood and severity of harm;
- containment already achieved; and
- other applicable legal or contractual requirements.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay where required by law.

If all information is not available within the initial reporting period, Paulioskos may provide information in phases and explain any delay where required.

8. Incident record

The incident record should contain, as applicable:

- discovery and awareness times;
- reporter and internal owner;
- systems/services affected;
- factual chronology;
- categories of information affected;
- approximate number of records/individuals affected;
- containment and recovery actions;
- credentials/tokens/certificates revoked or rotated;
- business and security impact;
- risk assessment;
- notification decision and rationale;
- regulator/HMRC ticket or reference numbers;
- communications issued;
- root cause;
- corrective/preventive actions; and
- closure approval.

Secrets and unnecessary personal information must not be copied into routine incident records.

9. HMRC credential and token response

Where HMRC credential compromise is suspected, the Finance Technical Owner will assess and, where appropriate:

- disable affected Finance/HMRC integration functions;
- revoke local authorisation;
- rotate the affected HMRC client secret;
- invalidate or replace token-encryption material where necessary;
- re-authorise only after the environment is trusted;
- confirm that no unauthorised API actions occurred; and
- validate fraud-prevention and OAuth configuration before returning to normal service.

Production credentials must not be moved into development or committed to source control during recovery.

10. Backup and recovery during an incident

Recovery must use trusted backups or known-good deployment artefacts.

Paulioskos Finance recovery planning protects more than source code and may include:

- PostgreSQL/application data;
- uploaded evidence;
- production environment configuration;
- certificates and private keys;
- HMRC token-encryption material; and
- other persistent state required for safe service restoration.

A recovery is not considered complete merely because the application starts. Data integrity, authentication, audit, HMRC connectivity and relevant security controls must also be validated.

11. Communications

Public or customer-facing communications should be:

- factual;
- proportionate to confirmed information;
- clear about what is known and not yet known;
- free of credentials, exploit-enabling details or unnecessary personal information; and
- updated where material facts change.

Paulioskos will not claim that an incident is resolved until containment and recovery have been sufficiently validated.

12. Post-incident review

Material incidents require a documented post-incident review covering:

- root cause;
- effectiveness of detection and response;
- whether controls operated as intended;
- whether backups and recovery were effective;
- any missed or delayed alerts;
- regulatory/compliance findings;
- lessons learned; and
- tracked corrective actions.

Changes identified by the review should enter normal controlled development/change management rather than being left as informal actions.

13. Testing and review of this procedure

This procedure is reviewed:

- at least annually;
- after a material Finance/HMRC security incident;
- before or after material HMRC production integration changes;
- following significant changes to hosting, authentication or backup architecture; and
- when HMRC, ICO or applicable legal requirements materially change.

Paulioskos may conduct tabletop or technical exercises to validate that the restricted internal runbook, contact information, credential-rotation steps and recovery procedures remain usable.

14. Public procedure and restricted runbook

This public procedure defines the commitments Paulioskos follows.

A separate restricted operational runbook contains implementation-sensitive information such as:

- named emergency contacts and telephone numbers;

- HMRC/ICO reporting links and account-specific details;
- system/host identifiers;
- exact credential and token rotation steps;
- backup locations and recovery commands;
- security tooling and log locations; and
- escalation contact trees.

The restricted runbook is not published because doing so could weaken security.

Contact

Route	Details
Security reports	security@paulioskos.com
Responsible disclosure policy	Open Responsible Disclosure Policy
Trust Centre	Open Trust Centre
Postal correspondence	Unit A, 82 James Carter Road, Mildenhall, IP28 7DE

Reference framework

These sources describe the legal, regulatory and good-practice framework used when preparing this document. They do not represent certification, accreditation, HMRC approval, regulatory endorsement or legal/tax advice.

Source	Link
HMRC Developer Hub - Terms of Use	Open source
HMRC - Test Fraud Prevention Headers API 1.0	Open source
ICO - Personal data breaches: a guide	Open source
Paulioskos Responsible Vulnerability Disclosure Policy	Open source
Paulioskos Trust Centre	Open source