

EXPIRY REPORT

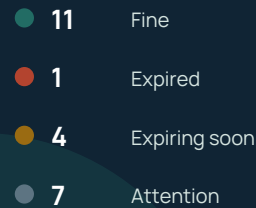
Executive summary

Tailspin Toys | 10 October 2026 | Internal assessment

OVERALL POSTURE

Expiries require attention

These figures cover the 23 items this run read; 0 ignored items stay out of them and are listed in the technical report, so its totals differ by design.



1

Already expired

11

Fine on the run date

4

Expire in 30 days

23

Watched items

The leading areas for review are App registration secrets and certificates, Intune certificates and tokens, enterprise application credentials. The run found 1 expired and 4 expiring within 30 days among 23 watched items. Days left are counted from the run date, not from today. The report does not establish that a renewal is under way unless the item was marked handled in the portal.

WHERE TO FOCUS

01

App registration secrets and certificates

2 items due · EXPIRED

02

Intune certificates and tokens

2 items due · SOON

03

Enterprise application credentials

1 item due · SOON

DATED ITEMS BY DAYS LEFT



RUN SNAPSHOT

COLLECTION

212 applications, 488 enterprise applications, 2 domains read

Read-only; run from the app

HANDLING

0 handled / 0 ignored

Decisions recorded in the portal

OWNERS

2 without an owner

Assign in Entra or the portal

COVERAGE LIMITS

1 part not read

Grant the permission, run again

SINCE LAST RUN

First run

No earlier run to compare

THE MANAGEMENT DECISION

Assign an owner to every open item, agree who renews what before each date, and keep the schedule running so the next expiry is a warning, not an outage. Ignored items stay on the report with their reason.

PRIORITIZED FINDINGS & RECOMMENDATIONS

Priority workstreams

Ordered by the nearest expiry. Who renews what, and when, remains the owner's review.

01 App registration secrets and certificates



EXPIRED

4 items; 1 expired, 1 within 30 days. Legacy ticketing: expired 11 days ago. Payroll sync: 8 days left.

Action Add a new secret or certificate in the app registration, update the integration that uses it, then remove the old one. The next run shows the new date.

Why it matters When an application's secret expires, every sign-in and integration through it stops at that moment.

The decision Ask the owner to add a new secret before the date and confirm it on the next run.

02 Intune certificates and tokens



SOON

5 items; 2 within 30 days. Apple MDM push certificate (the certificate Apple requires before devices can be managed): 5 days left. Certificate connector SRV-PKI01: 25 days left.

Action Renew in the Intune admin center under Tenant administration, with the same Apple or Google account that created the token.

Why it matters When an Apple or Google token expires, phones and laptops stop enrolling and can lose management.

The decision Renew with the same Apple or Google account before the date.

03 Enterprise application credentials



SOON

2 items; 1 within 30 days. HR portal SSO: 22 days left.

Action Renew the certificate in the enterprise application's single sign-on settings and upload the new one on the application's side before the old one ends.

Why it matters When a signing certificate expires, staff can no longer sign in to the application that relies on it.

The decision Ask the owner to renew it on both sides before the date.

PRIORITIZED FINDINGS & RECOMMENDATIONS

Supporting workstreams

Ordered by the nearest expiry. Who renews what, and when, remains the owner's review.

04 Applications without an owner

ATTENTION

2 items; 2 need attention. HR portal SSO: no owner. Intranet SharePoint connector: no owner.

Action Assign an owner in the Entra admin center or in the portal, so that Remind knows whom to warn before the next expiry.

Why it matters Nobody is warned about an item without an owner, so its expiry is found when something stops.

The decision Name an owner for each one now; it takes a minute in Entra or in the portal.

05 Unused applications

ATTENTION

2 items; 1 needs attention. Old CRM import: last sign-in 2026-03-02.

Action Confirm with the owner that the application is no longer used, then remove its credentials or the application itself.

Why it matters A credential nobody uses still opens a door, and if it leaks nobody notices.

The decision Ask the owner whether the application is still needed; remove it or its credentials.

06 Domains and mail records

ATTENTION

7 items; 3 need attention. tailspin-mail.example: DKIM (the signature that proves mail really came from the domain) not enabled. tailspin.example: SPF (the list of servers allowed to send mail for the domain) differs.

Action Correct the DNS record at the registrar to what Microsoft publishes and rotate DKIM in the Defender portal; check the next run after DNS has propagated.

Why it matters A wrong mail record means the company's mail bounces or lands in spam, often without a warning.

The decision Have the DNS host fix the record and check that the next run shows it as fine.

PRIORITIZED FINDINGS & RECOMMENDATIONS

Supporting workstreams

Ordered by the nearest expiry. Who renews what, and when, remains the owner's review.

07 Entra Connect and cloud sync

ATTENTION

1 item; 1 needs attention. Entra Connect (the service that copies on-premises accounts to Microsoft 365) sync: 2 sync errors.

Action Check the Entra Connect or cloud sync server: the service, the connector account and the last completed synchronization.

Why it matters If directory sync stalls, password changes and new staff do not reach Microsoft 365.

The decision Have IT check the sync server today; it is usually a stopped service or an account.

08 Conditional Access references

NOT READ

Not read in this run: This part was not read in this run: the Conditional Access (the sign-in rules of the tenant) permission was not granted. Run again with that permission to include it.

Action Grant the permission at the next run; the result is a coverage limit, not a pass.

Why it matters This part was not read in this run, so it gives no assurance either way.

The decision Grant the missing permission before the next run so that this part is included.

DELIVERY PLAN & ASSESSMENT CONFIDENCE

From findings to action

Proposed timing starts when the plan is accepted. Owners and exceptions remain to be agreed.

01

First 30 days

Renew everything already expired or due within 30 days. Assign an owner to every item without one. Record handled or ignored for each decision in the portal.

02

Days 31-60

Renew the items due within 60 days. Correct the mail records and the directory synchronization. Remove unused applications once their owners confirm.

03

Days 61-90

Set the schedule: daily runs, warning addresses per tenant and a review of ignored items. Close an item only when the next run shows its new date.

COVERAGE & DECISIONS

COLLECTION

Not read in this run: the Conditional Access policies. A part that was not read gives no assurance; grant the permission and run again.

CONFIDENCE

23 items were read from 212 applications, 488 enterprise applications and 2 domains on 10 October 2026. Days left are counted from that date. No trend is inferred without an earlier run.

BOUNDARIES

Remind reads the names and dates of credentials, never their values, and never renews anything. Secrets kept outside Microsoft 365, certificates on servers, third-party services and licenses are outside scope. DNS records are read from the computer that ran the app, so a split DNS can differ from what the Internet sees.

ACCEPTANCE

An ignored item stays on the report with its reason. A handled item returns to open when the next run still finds the old date after the expected date. Require an owner, a date and a note for each exception.

Sample report: fictional organization

This report lists the credentials, certificates, tokens and records read from the Microsoft 365 tenant named in it, at the time shown, within the limits in its coverage section. It is a point-in-time review, not an audit opinion, a certification or a guarantee that nothing else will expire or break. Days left are counted from the run date. Findings and guidance are informational; renewals are made by the customer, and nothing in this report changes a tenant. Parts that could not be read are reported as not read, not as fine. Microsoft behavior can change after the run date. Prepared by GlacierPoint Technologies LLC under the GlacierPoint Remind Terms of Service.