mimecast

Checklist for security during employee offboarding

A collaborative effort between HR, IT and Security

Departing employees present one of the highest insider threat risks. Therefore, it is essential that every company incorporate security during the offboarding process. This checklist can help you with that.

Stay in sync – HR, IT and security need to act as one from the moment a termination or resignation happens. That means they're notified simultaneously and they automatically kick-start a joint off-boarding process.

Check the rear-view mirror - The 90 days before a person leaves a company are a prime window for suspicious data activity. Incydr conducts an automatic historical analysis for every departing employee or contractor's file activity, so you can catch anything unusual in plenty of time.

Revoke access, transfer ownership – If the person leaving is a system admin, app owner or a vendor relationship owner, be sure to remove their access and transition ownership before they leave.

Make a list, check it thrice – Make a list of all the apps, systems, devices, tools, resources, fobs, keycodes and anything else departing employees have access to—ask their line-manager about any shadow footprint they know of.

Survey before exiting – Capture employee feedback and establish clear expectations post-employment. Why are they leaving? Is there a non-compete or non-solicitation clause? Do they understand all relevant acceptable use policies?

Get forensic – Validate your employees exit surveys with a risk-based analysis of their role, tenure, cyber-behavior, exit reasons and data access. If they're classifie-das high risk, pursue a more rigorous offboarding program.

Offboarding itself – Remember to track data behavior throughout the offboarding process itself (again, using something like the Incydr departing employee watchlist). Just because you didn't flag anything in the last 90 days doesn't protect you from any last-minute suspicious activity.

On their last day

✓ **Get it back** – Ensure all company property (especially devices and badges) is collected and returned to the right teams.

Shut it Down – Start the system-access shut-down process the moment the employee leaves.