

Secure IP Employee Offboarding

PROGRAMMATICALLY DETECT AND MITIGATE IP LOSS WHEN EMPLOYEES LEAVE YOUR ORGANIZATION

When an Employee Goes to Work for a Competitor, Your Valuable Company IP Shouldn't Go with Them

When employees leave your organization, you're at risk for more than just corporate brain drain. Departing employees can exfiltrate valuable intellectual property (IP), taking with them sensitive proprietary items like source code, strategy documents, contact lists, and financial information. You likely won't know it happened...until it's too late.

In fact, studies have shown that one-third of departing employees take IP with them—and whether it's for portfolio-building or to share trade secrets with a competitor, teams responsible for offboarding may not be well-equipped to know which employee has leaked data, or how much you've lost.

Employee offboarding has traditionally been siloed as an HR or IT function, where a series of gated steps ensure that systems access is removed, loaned hardware is reclaimed, and a departing employee is removed from payroll and the directory. Yet what often fails to make the checklist is an audit of the person's network activities during their last days of employment. You know they returned their laptop and badge—but can you also be sure about the IP they created and accessed during their tenure?

Lighthouse Can Help

Lighthouse's employee offboarding solution is designed to stop IP theft in its tracks, using remote interview and analysis sessions and state-of-the-art forensic technology to understand and analyze employees' activities in their final days of employment with your company.

Benefits

Proactive data security

Use proactive scoping and assessment to identify leaks before they cause monetary, operational, and reputational damage.

Seamless escalation

Move rapidly from light analysis to forensic collection, investigation, and review—with people and technology handoffs under one roof.

Controlled spend

Service pricing is based on interviews and reporting for a set number of departing employees per month, so there are no billing surprises.

Augmented expertise

Partner with Lighthouse forensics experts to layer data security on your existing offboarding process.



Scoping



Scan + Image



Report

Our experts work with stakeholders across your enterprise to properly assess the risk of certain classes of employees, whether based on role, circumstance of departure, seniority, or access to sensitive information.

After performing remote scans of departing employees' laptops and forensic analysis of assets and online behaviors, our digital forensics consultants generate a report of their findings for each exiting employee. The report presents our recommendations, which may include additional forensic investigation, and assigns risk levels to each artifact we analyze. You can also gain strategic insight by reviewing the corpus of reports to identify trends over time.

Get the Most from Lighthouse Employee Offboarding Services

Lighthouse offers additional services to ensure that IP security offboarding fits your enterprise-specific goals:

- Informational, low-pressure interviews with exiting employees
- Data loss prevention (DLP) log analysis
- Microsoft M365 insider risk management analysis
- In-place document preservation for legal hold or business continuity
- Coordination with outside counsel to attend remote offboarding sessions

Find Out More

Combining thorough risk scoping, remote scanning and imaging, employee interviews, full documentation of findings, and the ability to seamlessly escalate to investigation should the need arise, our employee offboarding solution reduces the risk of IP exfiltration—all at a predictable cost.

Reach out to your Lighthouse account executive to find out more about our offboarding services and how the Lighthouse approach can strengthen your existing risk and compliance programs.

Contact us to find out what Lighthouse can do for your business.

206-223-9690 | lighthouseglobal.com | info@lighthouseglobal.com



LIGHTHOUSE