# 9 Internal Security Culture Gaps

| Target Process | Target Asset | Impact |
|---|---|---|
| ALL | ALL | HIGH |

## EXAMPLES

- Licensee fails to establish the level of IP exposure required at each development stage, resulting in overexposure to risk for business needs.
- Licensee fails to onboard vendors and subcontractors with alignment on security requirements.
- Licensor or Licensee fails to accommodate the needed pathways for IP assets during development, resulting in overly restrictive workflows that impact business, causing "rogue" behavior to accomplish goals.
- Failure to restrict digital asset usage to established parameters results in duplicative saved and shared copies of sensitive files across numerous systems, hindering investigation when a leak does occur.
- Lack of documented procedures leads to delays in identifying and correcting process gaps, leaving sensitive IP exposed unnecessarily.

## PREVENTATIVE CONTROLS

- Licensee should assess all business processes involving sensitive assets regularly, to identify vulnerabilities and establish procedures to mitigate risk.
- Licensee should require all 3rd parties who will receive sensitive IP for development or promotional needs to adhere to minimum standards for handling sensitive IP that are comparable to the licensee's internal standards.
- Licensee should regularly provide interactive training material to all staff with access to sensitive IP.
- Licensee should maintain a comprehensive incident response plan that details steps to take in the event of an IP leak and assigns responsibility for those steps.
- Licensee should establish, document, and periodically audit against security procedures designed to restrict sensitive asset exposure to critical business needs.

## BEST PRACTICES

- Engage up to a leadership level in a comprehensive security program that is regularly reviewed, assessed, and updated to fit current needs.
- Create an Incident Response plan with roles spelled out for relevant stakeholders, defining out incident response by severity type, and response plans by chronology and ownership.
- Develop rider and contract language that details security requirements and alerting procedures for all business partners.
- Foster a practice of limiting any use of embargoed IP in the marketing value chain to a need-to-know basis.

## DETECTIVE CONTROLS

- Licensee should prioritize methods of handling physical and digital IP assets that allow for user traceability at an individual level.
- Licensee should engage technology to monitor and alert against unauthorized access to or misuse of digital IP assets.
- Licensor and Licensee should use online monitoring services for key words related to embargoed product.



CDSA
Content Delivery & Security Association