Safeguarding Against Inauthentic Candidates: Salesforce Supplier Requirements and Standards

This document contains standards for contingent workforce suppliers to ensure compliance and prevent such suppliers from hiring and onboarding malicious actors, particularly North Korean IT workers, who may pose a risk to clients such as Salesforce.

Purpose

The purpose of this Security Enablement mechanism is to establish ***clear requirements, protocols, standards*** for Salesforce suppliers regarding the threat presented by the Democratic People's Republic of Korea (referred to as North Korea). This Security effort provides established requirements and protocols for suppliers to better detect and prevent the hiring and onboarding of malicious North Korean actors who pose risks to the data, assets and systems of clients such as Salesforce. The guidance provided in this document originates from private and public sector advisories warning against the threat from North Korean Information Technology (IT) workers.

Background

North Korea dispatches thousands of highly-skilled IT workers around the world to generate revenue for the North Korean government. These IT workers take advantage of existing skill set demands to secure positions globally, predominately at Western companies. In most cases, North Korean IT workers provide false or stolen identities to represent themselves as U.S.-based individuals, but may actually work in North Korea, China, Russia, or other locations with close relations with North Korea. The remote work culture has made it easier for these workers to use counterfeited, altered, or falsified documentation to secure employment. They commonly use virtual private networks or leverage third-country IP addresses to obfuscate their physical location and appear as though they are connecting from locations less likely to raise suspicions. Additionally, U.S.-based facilitators may

collude with North Korean IT workers to support their efforts in exchange for financial incentives.

Supplier Expectations

Salesforce expects all contingent workforce suppliers to adhere to the following standards to improve the detection and prevention of North Korean IT personnel being inadvertently hired or contracted. A vendor's failure to adhere to these standards directly increases risk to Salesforce, which warrants business review and possible contract termination of the vendor relationship.

Standards

1. Closely validate submitted identity verification documents for any anomalies, inconsistencies, or forgery.
2. Verify the existence of any websites provided to establish the validity of accounts and enhance validation for any accounts that are no longer available online. Verify that accounts appearing to be recently created or changed are authentic.
3. Require video (with video turned on) interviews for ALL candidates to verify identity and discourage the use of background filters and blurring features.
4. Require all applicants to undergo more than one interview with the supplier, even for short-term contingent roles; if they claim residency near a supplier's work center, attempt in-person meetings.
5. Verify that identity is consistent across platforms, websites, resumes, and identification documentation. If inconsistencies arise, escalate to management for validation and/or immediately halt the hiring process when legally authorized to do so.
6. Do not authorize payments using virtual currency and require verification of banking information that corresponds to other identifying documents.
7. Verify employment and higher education history directly with the listed organization and not through contacts provided by the applicant.
8. Carefully validate any sudden requests to change identification, location information, and/or requests to work from other states, countries and timezones.

Reference documents

- U.S. Department of Justice, 23 Jan 2025. https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote
- Wall Street Journal. 5 Sep 2024. North Korean Spies Are Infiltrating U.S. Companies Through IT Jobs.
- Department of Justice. 18 Oct 2023. Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers.
- Recorded Future. 23 Sep 2024. Dozens of Fortune 100 companies have unwittingly hired North Korean IT workers, according to report.
- The Hacker News. 20 Oct 2024. North Korean IT Workers in Western Firms Now Demanding Ransom for Stolen Data.
- KnowBe4. 18 Sep 2024. North Korean Fake Employees Are Everywhere! How to Protect Your Organization.
- Department of Treasury. 16 May 2022. Guidance on the Democratic People's Republic of Korea Information Technology Workers.
- Australian Government Department of Foreign Affairs and Trade. 23 Aug 2023. Advisory on Democratic People's Republic of Korea (DPRK) Information Technology (IT) Workers.
- Google. 23 Sep 2024. Staying a Step Ahead: Mitigating the DPRK IT Worker Threat.
- Department of Justice. 8 Aug 2024. Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator

[1]

[1] Last Updated: May 2025