

ANOMALIX WHITE PAPER

Non-Employee Identity Management



Non-Employee Identity Management

Employee identities are typically the responsibility of the Human Resources (HR) department and usually stored in a designated HR system. Regardless of the underlying technology being used, there are standard processes and tools to manage employee identities as they move through the organization. These use cases include:

- The initial on-boarding and identity creation
- Corporate reorganizations
- Job transfers
- Off-boarding as they leave the organization

However, non-employee identities (contractors, vendors, consultants, interns, etc.) don't always have clear-cut processes and procedures to govern their identity creation and access. Vendor Management Systems (VMS) are designed to capture basic vendor information, not to manage individual identity lifecycles and their associated access. Many organizations struggle to manage these users; where a decentralized process, inconsistent standards and a lack of oversight present dangerous and costly operational and regulatory risks to the organization.

When an organization's non-employee identity process lacks structure and a true ownership reporting designation costly mistakes happen. Examples of these mistakes are:

- Active users created from multiple points of entry can lead to duplicate and orphan accounts
- Active users with inappropriate access or access that has not been approved
- Terminated users with active access to the organization's resources after they have left the organization

Common scenarios involve a request that gets submitted into the organization's request/ticketing system by a hiring manager. Since this request process is un-governed and unsupervised, the data that is captured can be insufficient and of differing standards. First Name/Last Name become an email address, Expiration Dates are 50 years in the future (if required at all) and instead of granting the minimum access required they are given the highest (SysAdmin/Root) privileges. This becomes a major security issue if the non-employees continue to have access to sensitive information after they have been terminated. These are exactly the types of accounts that hackers look for when trying to penetrate systems and steal data.

While it is commonplace for the responsibility to default to HR or procurement, neither of these departments have the tools, systems or strategies in place to effectively manage a non-employee population. Many HR departments struggle to keep up with organizational changes, acquisitions and the normal workload for employee management, all of which put stress on even the best Identity Access Management program. Managing non-employees and their ever-changing relationships within an organization can be a complex and time-consuming task.

The lack of the proper tools and technologies make non-employee management an afterthought, without a single department taking full and complete accountability.

As a result, organizations sometimes develop disparate, competing homegrown solutions to manage this population. These ad hoc solutions range from an Excel spreadsheet to a local database to customization of an existing HR/IAM solution. While these solutions may work temporarily with a smaller non-employee population, as the population grows these ad hoc solutions become more burdensome to manage and open organizations up to great risk.

The Anomalix solution provides a single repository, governed by a standardized business process to create and manage non-employee identities. Organizations are able to:

- Reduce time to productivity.
- Reduce the cost of managing access.
- Adhere with regulatory compliance mandates to reduce operational risk

The Anomalix solution can be hosted on premise or in the cloud. Features and advantages of this solution are:

1. Manual and automated (bulk-load) identity creation. The user interface can be customized and exposed to the appropriate business users.

- Leverage self-service as much as possible, relieving the management burden from central IT.
- Foster the notion that the business has a critical stake in managing non-employee user populations; an easy to use interface reduces the barriers to these management tasks.

2. Capture signed agreements such as Non-Disclosure, Non-Compete Agreements and other contractual forms that should be saved as Identity data to centralize any/all relevant identity data.

- Require data such as start and finish dates for non-employees that trigger notifications in advance of termination dates to identify if extended access is needed.

3. Change Request history of all actions taken, including a database audit log of all changes affecting Non-Employee Users.

- Provide the context needed to explain to internal and external audit groups why a specific access creation/removal happened.

4. When identity records are created/updated, it can be integrated with the existing Identity management system, triggering any relevant provisioning/deprovisioning activities.

5. This repository would act as the authoritative user source for an existing Identity Management system. Any organizational process is supported at the time of identity creation.

- a. Dependencies between the two systems are limited to where data is exchanged; this is a self-contained solution with no specific version dependencies, it is just another data source.



ANOMALIX

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144