

**<Company Name>**

**Cyber Security Team Blue Team XX**

**Recipient**:

<Recipient Name>

<Organization> , <Recipient Location>

**Date**: March X, 2025

**Subject:** Response to Request <Insert Request Title/Number>

Dear <Recipient/Team>,

Thank you for reaching out to our team. We have received the recent request # [request number] made to our team. We were asked to create [X number] of users for [Y purpose(s)], while ensuring adherence to standard procedures and policies to maintain security and usability. Below, you will find our report detailing the actions taken and the outcomes of this initiative.

Thank you,

Blue Team XX

Executive Summary

The task at hand was to ensure that the organization’s IT environment remains secure, efficient, and fully aligned with internal and external regulatory standards. This initiative was driven by the need to manage user access within the Active Directory (AD) system, safeguarding sensitive data and maintaining a compliant infrastructure.

As part of this effort, a set number of user accounts were created to meet specific business needs. This simple creation process ensured that each user was properly provisioned with the necessary roles and permissions for their respective duties.

To further safeguard the system, industry-standard security measures were applied as defined by the Center for Internet Security (CIS) under [Control 5: Account Management](https://www.cisecurity.org/controls/v8-1). This also included enforcing strong password policies, implementing multi-factor authentication, and setting up appropriate access controls as defined by our company standards. These actions were essential not only for preventing potential security breaches but also for maintaining compliance with regulatory requirements.

By incorporating regular monitoring and auditing of user activity, we ensured that the system could quickly identify any suspicious behavior. This proactive oversight helps mitigate risks before they become issues, while maintaining accountability within the organization.

The outcome was a more secure and resilient IT environment that balanced operational efficiency with stringent security requirements. As a result, the organization is better positioned to maintain secure access to its resources and protect sensitive information, ultimately supporting its broader strategic objectives.

Assets Affected

| Hostname | IP Address | Additional Notes |
| --- | --- | --- |
| Wherever AD is | AD IP address | Active Directory (AD) is a directory service that is used to manage and organize resources in a network, such as users, computers, and other devices. It provides centralized authentication, authorization, and management, helping ensure that only authorized users have access to the appropriate resources. |

Fulfilled Action Items

1. Generated users for X reason, under Y group. <Give screenshot below>
2. Enforced proper policies and standards (password complexity, MFA, etc.) <screenshot below>
3. Enabled auditing and tracking of user movement. <screenshot below>