Identity Policy  
NIST 800-63:

<https://pages.nist.gov/800-63-3/>

Section A: Enrollment and Identity Proofing   
  When onboarding a new user(s), how do we verify they are who they say they are.

Section B: Authentication and LifeCycle Management  
  How do users authenticate to a specified system? (UserName/Password, SSO   
  [Kerberos, SAML ...], )  
  Password rotation policy.

Section C: Federation and Assertion  
    <https://www.nist.gov/video/special-publication-800-63-3-public-draft-webinar>

Using the NIST 800-63 Sections A/B/C, develop an Identity Policy that will be   
used to create a login profile for your new users as well as a password/  
authentication device reset.  
Some situational context:  
For simplicity, your users are US based only, Hybrid work environment, they are   
NOT allowed to work remotely from OCONUS (Outside the Continental US).

You can find templates online for similar policies, therefore, you have the freedom in the format chosen, as long as it is well/clearly developed.

What to submit:  
1 - Upload the document to your Github profile.

2- Create a 10-15 minutes video explaining your policy and how it relates to the NIST 800-63 publication, then add the URL to your Github profile under the same project repo/Directory.

3- Submit the URL to your Github profile (the page should show the Policy as well as the URL to your youtube demo).

**My Policy**

Section A:

HR will filter candidates and verify legitimacy of the candidate by

Background Check, ID verification (Driver’s License or Passport and Tax Verification(W-9), Fingerprinting.

Having Fingerprinting as a requirement supports IAL 3 of the NIST SP 800-63A Standard and Having Background Check and ID verification supports the IAL 2 of the NIST SP 800-63A Standard.

Access then will be granted by the role of the user (Employee, Intern, Contractor).

Email and User accounts will be generated by the first letter of the first name and last name and have the role.

INT – Intern

EMPL – Employee

CONTR – Contractor

Ex: [smuralidharINT@company.com](mailto:smuralidharINT@company.com)

This setup process will be done in person – supervised in the office.

Section B:

Users will be verified by a Company issued Personal Identity Verification (PIV) card. The PIV card will be used to login into Work issued laptops along with the Users Username and password. This is to maintain high authenticity in the event the username or password is compromised. Additionally work-related applications such as Emails and work chats that are accessed via the browser will need a Token facilitated by the multi-Factor authentication to authenticate the User.

If password is forgotten, the User must contact IT support team and provide them with the 6-digit badge number located on their PIV number. Additionally, the IT team will send a token to their phone to verify identity.

Using Multi-Factor Authentication as requirement supports AAL 1 of the NIST SP 80063B Standard and requiring a PIV card to turn on work issued laptops supports AAL3 of NIST SP 80063B standard stating of the use of a hardware-based authenticator must be used to prevent verifier impersonation.

Section C:

For at-home / remote working users a VPN must be used to access company servers and resources. The recommended VPN will be Cisco AnyConnect.

Resources such as email and teams can be accessed without VPN. However, access to the serves must need a VPN. The VPN cannot be accessed on personal devices. It must be accessed only through company provided devices.

If users’ needs a mobile access. A separate company device other than the personal device will be needed to distinguish personal and work. Mobile communication such as teams and mobile email will only work on the company devices.

An Access Control List or ACL will be used to block any non-continental US IP address.

<https://www.countryipblocks.net/acl.php>

It is important to note that someone who knows how to use a VPN can bypass this by looking like it is coming from a different country. For example if I want to access an Indian only site from US I can easily do this by using a VPN.

SSO (Single Sign on) will only be used on browser access emails and will be active for 10 days using SAML (Security Assertion Markup Language).