External Login Guidance

Hennepin County staff should utilize this guidance to decide if authentication (aka login) is needed for a technological solution or application with digitally capable community members (i.e., residents, users, people served, vendor, visitor, external stakeholders). Conditions are prioritized sequentially, and all rows must be met within a column.

Authentication and login are used interchangeably in this document. The purpose is to create access to an account by a user.

Verification[1] and *authorization*[2] processes and determination are completed by Hennepin County lines of business with consultation and guidance from data security, compliance and IT architecture.

Conditions	Login Not Required	Login Optional for Resident	Login Required
Identify statute/ policy/ procedure/ standards[3]	• Statute requires anonymous submission options. • There are no rules, statutes, or business needs for digital authentication.	Business process provides verification and authorization needed for increased interaction through digital authentication.	Statute, policy or standards require digital authentication.
Assess data returned to external user	Users cannot receive non-public classified data.	• If not authenticated, users cannot receive non-public classified data. • If authenticated, users may receive non-public classified data.	Users can receive/retrieve non-public classified data where they authenticate and are verified.
Assess user value	• Individuals may submit non-public information through an approved distribution channel. • Low barrier to access public information.	Login may be advantageous for user experience and should return value to community member.	Provide a value return to community member.
Consider disparity, equity, and accessibility[4]	• Anonymous or guest experiences provide the lowest barrier for technical delivery. • Non-technical delivery of services should be available to complement digital services.	• Anonymous or guest experiences will lower the barrier for technical delivery. • Evaluate the overall service delivery process (technical and non-technical) to mitigate disparity, equity and accessibility considerations.	Evaluate the overall service delivery process (technical and non-technical) to mitigate disparity, equity and accessibility considerations.

Compiled in the summer of 2023 by a sub-committee of the Technology Policy Committee including representatives from the Office of Digital Experience, IT, Human Services and Resident Services. Endorsed by the Technology Policy Committee in November 2023.

For further guidance, consult the Office of Digital Experience and IT Identity and Access Management.

---

[1] *Verification* is defined as the process of confirming a person is who they claim to be and not someone else.

[2] *Authorization* is defined as allowing access to something.

[3] Examples include but are not limited to: HC Cybersecurity & Data Protection Program, HC Digital Accessibility Policy, NIST (National Institute of Standards and Technology), HIPAA, CJIS (Criminal Justice Information), and State of Minnesota (DHS, MDH, MNIT, DVS) guidance. Utilize the Tennessen warning when collecting data from residents.

[4] Digital service channels create opportunities for digitally capable users. Service channels must continue to exist for residents lacking access to digital skills and technology.