The Kronos System is an electronic time keeping system, utilized as a time clock system, by the Department of Health and Human Services and the Department of Correctional Services. The Kronos System is supported by the Office of the CIO. The Kronos Steering Committee is comprised of authorized representatives of each agency, who are empowered to make policy and operational decisions as it relates to use and support of the Kronos tools.

- **Agency name** - Kronos Steering Committee (NDCS/HHSS/OCIO)
- **Name, title, and contact information for the agency contact person regarding the request** - Robert Shanahan, IT Manager, NDCS 402-489-5809
- **Title of the NITC Standards and Guidelines document at issue** - Standard 8-301 *Password Policy*
- **Description of the problem or issue** – Kronos is currently out of compliance with the NITC Password Policy (and has been so since its inception) in the following areas;
    - Sequential character limitation – none
    - Contains three of four character types – not required
    - Case sensitive characters – not recognized
- **Description of the agency's preferred solution, including a listing of the specific requirement(s) for which a waiver is requested**
    - The Kronos Coordinating Committee with support of OCIO has implemented all aspects of the NITC 8-301 password standard for the Kronos Timekeeping System which are supported natively by the AS/400 operating system. (The AS/400 platform hosts the Kronos Timekeeping System). The Kronos Steering committee requests a waiver from the NITC 8-301 password standard, specifically;
        - NITC waives Standard 8-301 for the Kronos System, contingent on continued enforcement of the following minimum requirements for Kronos;
            - Passwords must contain at least 8 characters
            - Passwords must contain;
                - At least one (1) alphabetic character
                - At least one (1) numeric character
            - Passwords must change at least every 90 days
            - Passwords cannot be the same as any of the previous 32 passwords
- **Any additional information and justification showing good cause for the requested waiver**
    - Although Standard 8-301 includes no requirement that a system must be able to enforce the password criteria, the Auditor of Public Accounts says "it has been our office's position that we cannot verify that users are properly utilizing passwords that meet the criteria without an agency enforcing the criteria through password settings." Consequently, non-compliance with 8-301 has been a finding of recent Kronos audits.

- Approval of this waiver appears to be the only way to satisfy the Auditor, based on the position outlined above. (The alternative is to accept the expense of writing and maintaining custom code in order to achieve full compliance.)
- The Kronos system is not accessible outside of the state network – all users must first authenticate (using fully compliant passwords) to the network before gaining access to the Kronos system
- Kronos access control is reasonable and sufficient, and the additional security to be gained from custom coding is not cost justified.