Partnering with Department of Public Safety

Form Purpose

This form is to request accesses and role permissions for information technologies at the Department of Public Safety. It is intended for existing employees and DPS internal use.

The form may be used to

- add, change, or remove an individual's access to systems.
- add, change, or remove access to databases.
- re-enable a privileged account.

Open this form in Adobe Acrobat Reader. It may not function properly when opened within a browser.

For questions about this form, contact nancy.trusty@state.mn.us

Form Instruction

Requestor/User

1. Fill out the Requestor Information section.
2. Check the provided box(es) to choose the area(s) of access.
3. Fill out the applicable form section(s).
4. Click the button "Submit to My Supervisor/Manager."

Supervisor/Manager

1. If the request is approved, then sign, approve, and submit the form.
   a. Go to the "Supervisor or manager approval" section near the bottom of the form.
   b. Sign the form by entering your last name and first name.
   c. Check the "I approve" or "I do not approve" box.
   d. Click the button "Submit to Service Desk."
2. If the request isn't approved, inform the requestor.

Requestor Information

Note: A Supervisor or Manager must be a DPS or MN IT employee.

Last name	First name	Middle initial
Work phone	Work email	
Division	Position title	Username (if applicable)
Contractor or vendor Yes No	Company (if applicable)	Form submission date
Supervisor/manager's last name	Supervisor/manager's first name	Supervisor/manager's work email

Areas of Access

System access   Database access   For each area selected, provide needed information in the related section, below in this form.

Re-enable privileged account

System Access

Requested environment (check all that apply; name the system in the right column)

Production

Certification

Development

DMZ

Sudo

Access action   Requested effective date
   Add   Remove   Change

Access type   Requested end date
   Read   Read/Write   Administrator

*Effective period to be no more than six months for Development or two weeks for DMZ and Production troubleshooting

*See Identity and Access Management Standard, Control 12, Privileged Account Use

*See Secure Systems Development and Acquisition Standard, Control 13, Developer Access to Production

Re-enable privileged account

Account name (i.e., dev-jdoe, sa-jdoe)

Name the systems or applications that are in scope for this privileged account

Database Access

Database name   Applicable division

Object name (i.e., stored procedure, table, view)

Describe the data that is being accessed

Data protection   Data classification

Is this for a service (machine) access?   Yes   No

Requested environment servers (check all that apply; if known, name the server in the right column)

    Production (emergency request only, read-only access provided)
    What is the production issue being worked?

    Certification

    Development

    Sudo

Delete this account	Remove indicated access i.e., Windows remote, network drv	Add/change access i.e., Windows remote, network drv

Requestor login ID   Requested effective date   Requested end date

*Effective period to be no more than six months for Development or two weeks for DMZ and Production troubleshooting
*See Identity and Access Management Standard, Control 12, Privileged Account Use and Control 39, Database Access
*See Secure Systems Development and Acquisition Standard, Control 13, Developer Access to Production

Access privilege

    Read   Write   Execute   Other

Reason for Access Request and Details

Explain the need for this request and provide any other information helpful for fulfilling this request

Supervisor or Manager Approval

All access to systems or data, other than read only access to data with a data protection categorization of Low, must be controlled through the use of identification and authentication mechanisms. This access control must:
- assign privileges to individuals based on the individual's job classification and function.
- restrict privileges to the least needed for the individual or service to perform their role.
- deny all access that is not explicitly granted.
- remove all system access not explicitly required.

Last name   First name   Comments

I am the DPS / MN IT supervisor or manager for the person identified in Requestor Information.

    I approve   I do not approve   Date approved

*Effective period to be no more than six months for Development or two weeks for DMZ and Production troubleshooting

*See Identity and Access Management Standard, Control 12, Privileged Account Use and Control 39, Database Access

*See Secure Systems Development and Acquisition Standard, Control 13, Developer Access to Production

MN IT Administration

This section is for administrative purposes only. The Technology Access Control Team member identifies and contacts the data owner for access approval.

Service Desk ticket number   Access Team member last name   Access Team member first name

Date of data owner contact   Data owner last name   Data owner first name

Method of contact with data owner   Data owner decision   Date access granted
                                        Approved   Not Approved

Comments