MINNESOTA IT SERVICES

# ACCESS AND DATA REQUEST FORM

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 |
|---|---|---|
| Barton | Rayah | A |

| Work phone | Work email | |
|---|---|---|
| 651-201-7759 | rayah.barton@state.mn.us | |

| Division | Position title | Username (if applicable) |
|---|---|---|
| MN IT Services | ITS4 -Business Analyst | rbarton |

| Contractor or vendor | Company (if applicable) | Form submission date |
|---|---|---|
| ○ Yes ◉ No | | 12/15/2023 |

| Supervisor/manager's last name | Supervisor/manager's first name | Supervisor/manager's work email |
|---|---|---|
| Bounds | Lori | lori.bounds@sate.mn.us |

## Areas of Access

- [x] System access
- [x] Database access
- [ ] Re-enable privileged account

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

## System Access

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

| | |
|---|---|
| [x] Production | P2PR reporting services (read only) |
| [x] Certification | PSPR application and associated reporting services (Admin for TEST and CEF |
| [ ] Development | |
| [ ] DMZ | |
| [ ] Sudo | |

Access action

(•) Add ( ) Remove ( ) Change

Requested effective date

12/15/2023

Access type

( ) Read ( ) Read/Write (•) Administrator

Requested end date

12/31/2024

*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: TRI

Applicable division: Homeland Security and Emergency Manageme

Object name (i.e., stored procedure, table, view): Application and report server

Describe the data that is being accessed: Data about facilities and hazardous materials they are storing

Data protection: Low

Data classification: Public

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) | Reporting server- read only |
| What is the production issue being worked? | Reporting questions |
| ■ Certification | Regular site access, admin site acce |
| ☐ Development | |
| ☐ Sudo | |

| Delete this account | Remove indicated access i.e., Windows remote, network drv | Add/change access i.e., Windows remote, network drv |
|---|---|---|
| ○ | ○ | ◉ |
| | | N/A |

| Requestor login ID | Requested effective date | Requested end date |
|---|---|---|
| rbarton | 12/15/2023 | 12/31/2024 |

*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

The application support team needs this access to respond to requests for support and development

**Submit to My Supervisor/Manager**

## 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

**Submit to Access Control Team**

## 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 ◯ Approved ◯ Not Approved | Date access granted

Comments