

Access Management Policy

Revision: *Initial Release*

Effective: 2026-02-09

UNCONTROLLED COPY: ALWAYS VERIFY REVISION

<https://itservices.machspec.com/policies>

1 Purpose

The purpose of the Access Management Policy is to define the level of access each user has to company-owned or managed information systems and the data in Machine Specialties' systems. This policy document describes the general access rules for all company-owned or company-managed information systems.

2 Scope

The Access Management Policy applies to the following:

- All Employees of Machine Specialties
- All Contractors of Machine Specialties
- All vendors / third-party / visitors who temporarily access Machine Specialties' equipment
- All information systems of Machine Specialties
- All data repositories of Machine Specialties

3 Definitions

Privileged Account

An account authorized to perform administrative, system-level, or security-related functions

User Account

A standard account with permissions necessary to perform routine job functions. Does not include administrative, system-level, or security-relevant permissions.

4 Policy

Machine Specialties shall implement the principle of least privilege and role-based access control within logical access control mechanisms so that only authorized users can access company systems and data.

4.1 Types of accounts

All information systems must have one or many of these account types. It is the policy of Machine Specialties that the principle of least privilege shall apply to the provisioning of all access rights. That is, access to information, networks, systems, technologies, and facilities is provided to employees, subcontractors, supplier partners, customers (collectively users) only to a level and scope necessary to perform assigned duties and/or to fulfill contracted services.

4.2 General User Access Management

- All employees, contractors, and third-party users shall be assigned a unique identifier.
- Each information system should define, document, and implement its access management covering all aspects of the user lifecycle from onboarding to offboarding.
- Credentials used for accessing each information system must be provisioned and used in accordance with the credential policy.
- Each information system must implement the principle of least privilege, ensuring that the access rights to the users are minimum and required to perform the tasks expected of the users.

4.3 User Onboarding

- HR must notify IT of new hires or position changes requiring user access changes at least 72 hours before those changes need to occur. This notification must include the employee's role, information systems they will need access to, what functions the user will be required

to perform. Additional access required for the employee's job duties must be requested by the employee's supervisor.

- All new employees must participate in basic cybersecurity training before becoming an authorized user of the information system.
- Employees or users must request access to department-level information systems to the appropriate department manager, who must approve access to department-level information systems.
- Special privilege requests must be submitted based on the new employee's role to the appropriate information system owners.
- Elevated access must have manager approval and must be strictly reviewed and only provided if the user's duties require it.

4.4 User Offboarding

- A responsible party must revoke terminated employee's access by the end of the day of the employee's last working day at Machine Specialties, and verify that access has been removed. The responsible party is typically the IT department, but may include a delegated administrator of a company information system.
- System owners must regularly review access and remove orphaned or terminated employee's accounts
- HR must notify IT of employees leaving the company at least 72 hours before the employee's last day of work, if this date is known. For sudden departures, HR must notify IT as soon as possible.

4.5 Privileged Accounts

- **Privileged accounts** must not be used when accessing non-security functions.

- Users with both privileged and non-privileged accounts must use separate authentication mechanisms for each account¹.

4.6 Third Parties / Contractors

- All-access requests for contractors and partners should follow the same process as mentioned in the sections above.
- Access for third-party workers, contractors, and partners must be enabled for the approved period during which their partnership agreement or contract is valid.
- Remote access to third-party contractors must be provided only after a formal request.

4.7 Password and other authentication mechanisms

- All information systems must enforce a login with password requirements as defined in the credential policy document. 2FA authentication methods, hardware tokens and SSO may be used in place of a user password as defined in the credential policy.

4.8 Audits and Logs

- All user access to information systems must be logged.
- At the minimum, logs must contain the unique Id that can be linked backed to a system user.
- All logs must be stored according to the Logging and Monitoring policy

5 Enforcement

The access management policy is enforced by the Director of IT or designated individual.

Noncompliance and violations to this policy will be dealt with according to the sanctions policy.

¹Separate keys on the same physical smart card count as a different authentication mechanism.

6 History

Date of Change	Revision	Responsible	Summary of Change
2026-02-05	-	Billy Johnson	Initial release