IOTECH SOFTWARE	**PRIVILEGE AND USER RIGHTS MANAGEMENT POLICY**	Doc. Number	**POL.12**
		Release Date	**02.01.2024**
		Rev. Number	**00**
		Rev. Date	**--**

PRIVILEGE AND USER RIGHTS MANAGEMENT POLICY

1. Purpose

To define the rights and rules of privilege for users within the institution.

2. Scope

This policy applies to all users and units utilizing information processing resources.

3. Sorumlular

All senior management is responsible for ensuring that all employees act in accordance with this policy.

4. Implementation

Privilege Management

Privileges are limited to folder access, software installation, connection durations, network settings, general internet usage, guest internet access, and remote work/access. These are reviewed at least once every 12 months, and reauthorizations are conducted due to employment, termination, or role changes.

Privilege Management for Senior Managers

The request is sent to the manager. She or he sends an approval letter to the system administrator to fulfill the request.

Privilege Management for Institutional Staff

- The employee submits the privilege request to their supervisor.
- If the supervisor approves, the request is sent to the manager.
- The manager evaluates the request and, if deemed appropriate, sends an approval letter to the Information Technology Service Provider for the privilege.
- The privilege access right is granted for the duration deemed appropriate by the manager. At the end of this period, the right is removed by the Information Technology Service Provider**.**

Privilege Management for Service Providers

- The relevant supervisor of the service provider makes the privilege request.

- The request is sent to the manager.
- The privilege access right is granted for the duration deemed appropriate by the manager. At the end of this period, the right is removed by the Information Technology Service Provider.

5. User Rights

Software Installation

- The storage or installation of non-work-related software (including installation files) is prohibited under all circumstances.
- Users cannot install software on their computers without the manager’s approval, even if technically possible, as it may violate copyright laws and cause technical issues.
- If work-related software installation is necessary, the opinion and approval of the Information Technology Service Provider must be obtained.
- Software such as security analysis tools and system management tools can only be installed on computers and workstations by the Information Technology Service Provider, with the manager’s approval.
- The installation and use of utility system programs are only allowed for the information technology department.
- Utility system programs are only installed and used to resolve user issues and are not used in system management.
- In very special cases where remote work with restricted access is necessary, utility system programs can be used. In this case, a request must be made and the manager’s approval obtained.
- Once the task is completed, the utility system program must be terminated immediately.
- The usage durations of the software are agreed upon with the relevant software owners and applied to the groups defined within the domain.

6. Configuration and Security Settings

Users cannot lower the security settings on their computers, even if technically possible.

Examples of security settings include:

- Security zone settings affecting MS Internet Explorer and MS Outlook,
- Virus protection program settings,
- Operating system update settings,
- Personal firewall settings,
- BIOS settings and other hardware and software security settings.

- Users cannot run new network services (such as web servers or database servers) on their personal computers, even if technically possible.
- Users cannot create new users and user groups on their computers, nor change the rights and groups of existing users.
- If configuration and security settings need to be changed, the opinion and approval of the Information Technology Service Provider must be sought.
- Configuration and security settings changes can only be made by the Information Technology Service Provider and only for the necessary period.

7. **Access Rights to Networks and Network Services**

- Users' access rights within our company are restricted to their own department’s area.
- Access restrictions are managed with Active Directory.
- Authorization schedules regarding access restrictions have been created, maintained, and reviewed following employment changes.
- Access to printers and similar resources over the network is configured by the Information Technology Service Provider.
- Access to applications on other sub-networks over the network, if needed, is configured by the Information Technology Service Provider.
- Local administrator privileges, except for the “power user/local admin” group, have been removed.
- Inclusion in the power user group is for the duration defined by the manager.
- To gain power user group rights, the user must first request it from their administrative supervisor. If the administrative supervisor approves, they will discuss it with the Manager.
- If the manager approves the request, a record is created via the help desk for the Information Technology Service Provider.

8. **Document Access Rights**

- Upon notification of a role change from the Human Resources department, the access settings for the current department folder must be removed, and access settings for the new department folder must be configured.
- For new personnel, a written (email) request must be received from the human resources department regarding which folder and folder access permissions are required. Without a written request, no access permission changes are made.
- The Information Technology Service Provider is responsible for checking and authorizing the document access permissions of all computer users at least once every 12 months and during role changes.

9. **Folder Access Permissions**

- Access to the IOTECH “Yeni ORTAK” is configured to allow only users included in the domain infrastructure.

- Department folders are fully accessible to the users of that department, and access permissions to other department folders are granted based on the manager's approval.

10. Device Usage

- Under user rights, all users’ USB ports (external disks) are disabled. If necessary, authorization is granted by the Information Technology Service Provider for a limited time and quantity with the approval of the relevant manager.
- If use is mandatory, usage rights are granted according to privilege management. The user is responsible.
- Consultants, customers, and visitors are not included in the institutional network.
- The use of service providers’ devices is subject to permission, and privilege management is applied.
- The “device identification policy” is active within the domain. A log is kept for each connected device.

IOTECH YAZILIM SANAYİ VE TİCARET ANONİM ŞİRKETİ