# Administrative Rights Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The granting of administrative rights to an employee of [Company Name] over an individual desktop, laptop, or other end-user device is a privilege only awarded to individuals who require this level of access and control in order to do their jobs effectively. The goal of this policy is to describe the circumstances under which administrative rights can be granted as well as the terms and conditions upon which this privilege will be granted.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This policy applies to all employees of [Company Name] and information technology machines owned by [Company Name].

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

The granting of administrative rights allows the individual to change the configuration settings of a given machine and install software on that machine. As a result, these rights can expose the [Company Name] network to malware and other security exploits. In addition, incorrect configuration of machines can lead to performance problems, potentially resulting in machine downtime, lost productivity, and higher support costs.

Given the serious consequences of mishandling or abuse of administrative rights, these rights will only be granted under the condition that they are essential for the performance of the grantee’s job. Such conditions could include the following:

* The ability to download and install specific types of software or configure system settings is mandated in the individual’s job description.
* An administrative rights access level is required for a necessary software title to run on a given machine. Company-owned and supported titles to which this applies include:
	+ [Software title and version]
	+ [Software title and version]
	+ [Software title and version]
* Sufficient levels of IT support do not exist due to time-of-day, geographical, or expertise constraints.

Typically, the only individuals at [Company Name] who are granted administrative rights include:

|  |  |
| --- | --- |
| **Job Title** | **Requirement for Administrative Rights** |
| Desktop Support Technician | Set up desktops and laptops for end users. Provide desk-side and remote support to desktop and laptop users.  |
| [Job title] |  |
| [Job title] |  |
| [Job title] |  |
| [Job title] |  |
| [Job title] |  |
| [Job title] |  |
| [Job title] |  |

**Note:** Members of the IT Department are not automatically granted administrative rights based on their membership in the IT Department alone.

If you do not hold one of the job titles described in the table above, then you will need to apply and gain approval for administrative rights if you believe it is required by your job. To apply for administrative rights, please use the Administrative Rights Application Form located at the end of this policy document. The designated authorities of the IT Department reserve the right to deny the application if it does not represent a clear business need or if the applicant has a documented history of security policy violation.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Administrative Rights Application Form

|  |  |
| --- | --- |
| **Employee Name** |  |
| **Employee Job Title** |  |
| **Employee Department** |  |
| **Employee Phone/Email** |  |
| **Supervisor** |  |
| **Date of Application** |  |

Please provide the following information:

|  |
| --- |
| Identity of machine for which administrative rights are being requested. |
|  |
| Reason that administrative rights are required. |
|  |

**Supervisor Approval**

I approve the request for administrative rights as outlined above.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor Signature Date

**IT Approval**

**This section is for IT Department administrative purposes only.**

The request has been: \_\_\_ Approved \_\_\_ Denied

If the request has been denied, please document the reason for denial.

|  |
| --- |
|  |

If the request has been approved, please document the following information:

|  |  |
| --- | --- |
| **Planned Activation Date** |  |
| **Actual Activation Date** |  |
| **Policy Read and Signed** |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT Authority Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT Authority Signature Date