# Third-Party Access 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 purpose of the [Company Name] Third-Party Access Policy is to establish the rules for third-party access to [Company Name] information systems and the computer room, third-party responsibilities, and protection of [Company Name] information.

# 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.

The [Company Name] Third-Party Access Policy outlines responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of the [Company Name] personnel responsible for the contracting and/or supervising of the third party. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

# 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.

1. All third-party access to the computer room should be scheduled to occur during regular business hours. If this is not possible, a point person from the IT department will be scheduled after hours to accompany the third party.
2. When third parties are scheduled to have access to the computer room, the Information Technology Services staff must be notified in advance of the date, time, and type of work to be performed.
3. When the third party arrives, he/she will report to a staff contact that scheduled the visit. The staff contact will escort the third party to the Information Technology Services area. At this point, the third party is to be informed that he/she will take further direction from the IT staff point person in relation to their activity in the computer room.
4. Prior to the onset of any work, the third party will describe the activities that are planned.
5. The IT staff point person is responsible for explaining what measures need to be taken to protect the computer hardware and software, explain protective measures to the third party, and ensure that the measures come to fruition. In an attempt to offset delays in the work of the third-party individual(s), the IT staff will attempt to minimize the delays within the constraint of safeguarding the systems. The third party will need to clearly understand that they are to allow time for the IT staff to do what needs to be done to protect the computer systems before starting their work.
6. The third party will report to and receive instructions from the IT staff point person regarding their work in the computer room. The IT staff point person will also be kept informed of the status of the work, as well as the notification that the work is completed before leaving the area.

**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.

1. Any third-party agreements and contracts must specify:

* The work that is to be accomplished and work hours, any configuration information of any installed software, as well as virus checking of that software.
* The [Company Name] information that the third party should have access to.
* The minimum security requirements that the third party must meet (i.e. method for remote access).
* How [Company Name] information is to be guarded by the third party. Signing of a non-disclosure agreement is typically required.
* Strict use of [Company Name] information and information resources for the purpose of the business agreement by the third party. Any other [Company Name] information acquired by the third party in the course of the contract cannot be used for the third-party’s own purposes or divulged to others.
* Feasible methods for the destruction, disposal, or return of [Company Name] information at the end of the contract.
* The return of company property such as a laptop, PDA, or cell phone after the completion or termination of the agreement.

1. The third party must comply with all applicable [Company Name] standards, agreements, practices and policies, including, but not limited to:

* Acceptable use policies.
* Software licensing policies.
* Safety policies.
* Auditing policies.
* Security policies.
* Non-disclosure policies.
* Privacy policies.

1. [Company Name] will provide an IT point of contact for the third party whether it is one person from the IT department or an interdepartmental team. This point of contact will liaise with the third party to ensure they are in compliance with these policies.
2. The third party will provide [Company Name] with a list of all additional third parties working on the contract. The list must be updated and provided to [Company Name] within […] hours of any staff changes.
3. Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with the [Company Name] Password Policy. Managing connectivity with partner networks can be handled in different ways depending on what technologies are in place (i.e. encryption, intrusion detection, DMZ architecture).
4. Any third-party computer/laptop/PDA/tablet PC that is connected to the [Company Name] systems must have up-to-date virus protection and patches. The third party will be held accountable for any damage that occurs to [Company Name] in the event that an incident occurs.
5. If applicable, each third-party, on-site employee must acquire a [Company Name] ID badge that must be displayed at all times while on the premises. The badge must be returned to [Company Name] upon termination or completion of a contract.
6. Each third-party employee that has access to [Company Name] sensitive information should be cleared to handle that information.
7. If applicable, an explanation of how [Company Name] information will be handled and protected at the third party’s facility/site must be addressed.
8. Third-party employees must report all security incidents to the appropriate [Company Name] personnel.
9. If third-party management is involved in [Company Name] security incident management, the responsibilities and details must be specified in the contract.
10. The third party must follow all applicable change control procedures and processes.
11. All software used by the third party in providing service to [Company Name] must be properly inventoried and licensed.
12. All third-party employees are required to comply with all applicable auditing regulations and [Company Name] auditing requirements, including the auditing of the third-party’s work.
13. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the appropriate [Company Name] management.
14. All third-party maintenance equipment on the [Company Name] network that connects to the outside world via telephone lines, leased line, or the network will remain disabled except when in use for authorized maintenance.
15. The third party’s major accomplishments must be documented and available to [Company Name] management upon request. Documentation should include, but is not limited to events such as:

* Personnel changes.
* Password changes.
* Project milestones.
* Deliverables.
* Arrival and departure times.

1. Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to the company or destroyed within […] hours. The third party will also provide written certification of that destruction within […] hours. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by authorized [Company Name] management.
2. [Company Name] will perform an impact analysis of other business-critical functions, once work has begun by the third party.
3. [Company Name] will monitor system and network log files […] times per week/day.
4. [Company Name] will eliminate third-party physical access to facilities after the contract has been completed or terminated. The following steps must be performed:

* Remove third-party authentication and all means of access to systems.
* If needed, make sure that incoming email is re-routed to an appropriate person.
* Archive any third-party software configuration, and transfer ownership to designated internal staff.
* Get a written statement from the third party that any software created and/or installed by the third-party is free of viruses and any other malicious code.

# 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.