# Security Infrastructure 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.

Dedicated security infrastructure allows information systems to be provided a greater level of security than can be achieved through configuration control alone by delivering enhanced security capabilities. Without dedicated infrastructure, the potential exists that security vulnerabilities that cannot be mitigated by the capabilities inherent in [Company Name]’s information systems will be exploited leading to compromise of information system security.

# 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 Security Infrastructure Policy applies to all dedicated security systems that are deployed to protect the property of [Company Name]. Specifically, it includes:

* All perimeter protection platforms (i.e. firewalls).
* All malware protection platforms (i.e. anti-virus, anti-spyware, etc.).
* All intrusion protection platforms (i.e. intrusion detection).
* All data protection platforms (i.e. content filters, encryption).
* All other dedicated security systems [indicate platforms].

# 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. Boundary network access points will be protected by boundary protection systems (generally a firewall) that monitor and control communications. These systems will be configured to deny communications by rule and allow by exception, to prevent public access to internal networks, and to place controls on publicly accessible systems.
2. Boundary network access points will be protected by monitoring and/or intrusion prevention systems that monitor events, detect attacks, and provide identification of unauthorized information system use. These systems will be configured to monitor both inbound and outbound communications.
3. All information systems will be protected by malware protection systems where such solutions exist for the information system. At a minimum, malware protection will be performed at the network boundary, on email and other communications systems, and on all workstations, servers, and other endpoints.
4. Boundary network access points as well as all information systems will be protected by data protection platforms that monitor, control, and restrict the flow of data into and out of systems and into and out of networks. These platforms will include data encryption, session encryption, and content filtering.

**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.

**Procedure 1**

Appropriately configure and maintain information security infrastructure:

* + - * + Firewalls will be configured to block by default and allow by exception in regards to both inbound and outbound traffic:

*[Indicate required rules]*

* + - * + Anti-malware will be automatically updated on a daily basis or as frequently as is possible based on the distribution of patch and definition files from the anti-malware provider. Patches and updates will be centrally managed and distributed.
				+ Intrusion detection/prevention systems will be configured to monitor all inbound and outbound traffic, scanning for anomalous traffic signatures, and anomalous traffic patterns. These systems will be configured to issue alerts should inappropriate traffic be detected rather than take automatic action to resolve potential threats.
				+ Data protection mechanisms will be configured to monitor and restrict the flow of confidential and otherwise sensitive data:

*Content filtering systems will be configured to restrict the inbound flow of data*.

*Data leakage prevention systems will be configured to restrict the outbound flow of data***.**

*Data encryption systems will be configured to encrypt all portable devices, all backup devices, and all data stores that house confidential or otherwise sensitive information. These systems will be centrally managed and will provide centrally managed key escrow.*

# 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.