

(1.1.1) Executive Summary

Purpose	<p>This <i>policy</i> provides direction for the development of information security measures at the Principal Financial Group® (The Principal®) and is intended to define the controls used to safeguard information from unauthorized or accidental modification, destruction, and/or <i>disclosure</i>, and to ensure information is available and usable as needed to conduct business.</p> <hr/>
Scope	<p>This <i>policy</i> applies to:</p> <ul style="list-style-type: none">• All Principal Financial Group <i>information assets</i> worldwide.• All technical platforms (e.g., mainframe, mid-range, microcomputer).• All <i>personnel</i> who have a business relationship with The Principal, including, but not limited to, regular and temporary employees, customers, suppliers, contractors, agents, brokers, and business partners. <hr/>
Corporate Technology Policy Statement	<p>Information is a company asset and must be managed to ensure its <i>confidentiality, integrity</i>, and availability for <i>authorized</i> business activities. All information must be safeguarded against unauthorized modification, <i>disclosure</i>, or destruction, using controls that are commensurate with its value.</p> <p>The Principal Financial Group management shall ensure that the requisite levels of <i>information asset</i> protection are provided through compliance with this <i>policy</i>.</p> <hr/>
Responsibility for Policy	<p>The Chief Information Officer (CIO) of The Principal is the final authority for Corporate Technology Policies.</p> <p>The Head of Information Services is responsible for development, maintenance, implementation, operation and enforcement of Corporate Technology Policies.</p> <hr/>
Effective Current	<p>December 19, 2001 December 19, 2001</p> <hr/>
References	<p>None.</p> <hr/>

(1.1.2) Table of Contents

(1.1.3) Information Organization	3
(1.1.4) Service Restrictions	3
(1.1.5) Policy Violations	3
(1.1.6) Responsibility for Policy	3

(1.1.3) Information Organization

This information is organized by *policies* and *standards*. *Procedures* and work instructions will be added during a later phase of this project.

- *Policies* are a broad statement of principle or intent which presents management position. Policies are interpreted and supported by standards. Policies are global, mandatory, and long-term in nature.
- *Standards* are a rule which specifies a particular course of action or response to a given situation. Standards are global and mandatory directives for implementing management's policy to ensure compliance.
- *Procedures* are a plan of action that specifies how a standard or guideline will be implemented in an organization. Procedures for implementing standards or guidelines are developed by the business unit and are separate from this document. Procedures are local in nature and include detailed steps for performing job tasks.
- *Work Instructions* are instructions for each *area* that define each individual's responsibility. Each *area* is responsible for developing work instructions.

Glossary terms are italicized throughout the Corporate Technology *policies* and *standards*.

(1.1.4) Service Restrictions

Users of Principal Financial Group systems are expected to work responsibility, comply with local and countrywide laws, and *policies* of The Principal. Access to Principal Financial Group systems is a privilege that may be wholly or partially restricted by The Principal without prior notice and without the consent of the business area or user when required by and consistent with law; when there is substantiated reason to believe that violations have taken place, or, in exceptional cases, when required to meet critical operational needs. Such restrictions are subject to established procedures or, in the absence of such procedures, to the approval of the head of Corporate Information Services.

(1.1.9) Policy Violations

Violations of this policy may result in disciplinary action up to and including immediate termination of employment and legal prosecution.

(1.1.10) Reporting a Violation

It is the responsibility of each worker to report any known or suspected violations of this *policy* to the Information Security Officer. Failure to report a violation of this *policy* may also be considered a violation.

End of policy