INTERNET
SECURITY
ALLIANCE

CONTRACTING FOR INFORMATION SECURITY IN COMMERCIAL TRANSACTIONS

An Introductory Guide

Supported by

ISSA®

Information Systems Security Association

This publication is for informational purposes and does not contain or convey legal advice. The information in this publication should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

Participation in the development of this publication does not represent an endorsement of the content provided herein on the part of any specific company or corporation.

Additional copies of this publication can be purchased for $29.95 from:

Jennifer Johnson
Director of Marketing and Finance
Internet Security Allliance
2500 Wilson Boulevard Arlington, VA 22201-3834
United States of America
(t) 703 / 907-7708 (f) 703 / 907-7093
www.isalliance.org • jjohnson@isalliance.org

Internet Security Alliance Board of Directors List

Founders

Dave McCurdy
President
Electronic Industries Alliance

Alan Woods
Vice Chairman & CIO
Mellon Financial

Rich Pethia
Director of CERT/CC
Carnegie Mellon University

Executive Committee

Chairman
Ken Silva
CIO
VeriSign

Immediate Past Chair
Bill Hancock
EVP
Secureinfo Corporation

First Vice-Chair
Ty R. Sagalow
President, Product Development
American International Group

Second Vice-Chair
Bob Severson
Sr. Vice President,
Business Technology
Ceridian

Secretary/Treasurer
Sagar Vidyasagar
Executive VP (Advanced Technology)
Tata Consultancy Services

Board of Directors

Internet Security Alliance
2500 Wilson Boulevard
Arlington, VA 22201-3834
United States of America
(t) 703 / 907-7708 (f) 703 / 907-7093
www.isalliance.org

Contracting for Information Security in Commercial Transactions—

An Introductory Guide

A publication of the

Internet Security Alliance

Contracting for Information Security in Commercial Transactions — An Introductory Guide

Preface

Contracting for Information Security in Commercial Transactions—An Introductory Guide is a product of the Model Contract Project, a special development effort conducted by the members of the Internet Security Alliance, a leading voice for providing private sector leadership in improving global information security. For further information, see www.isalliance.org.

This Guide has been developed through the ongoing collaboration of a team of professionals drawn from inside and outside the membership of the Internet Security Alliance. While drafts of this Guide have been circulated and reviewed by many ISA members, the following individuals deserve special recognition: J. Michael Hickey – Verizon; Jim Trovato – Intuit; Ty R. Sagalow and Robert Roche – American International Group; Dan Akman – National Association of Manufacturers; Rick Ochman – Mellon Financial; Michael Hayes – Nortel; and John Shaughnessy – VISA.

The Model Contract Project has been supported by the international law firm of Kirkpatrick & Lockhart Nicholson Graham LLP (www.klng.com). Their lawyers served to collect and analyze significant, divergent sources of information and membership submissions and have been invaluable in developing the final version of this Guide. Jeffrey B. Ritter, resident in K&LNG's Washington office, served as the Reporter for this project; he was assisted by Bruce H. Nielson and Benjamin S. Hayes of K&LNG and by David K. Gaston, class of 2006, Harvard Law School.

In addition, Steve Roberts, an ISA staff member, provided ongoing support to the administration and execution of this work. These acknowledgements would not be complete without recognizing the stewardship of Larry Clinton, our executive director, whose gentle hand of leadership helped assure the completion of this work.

Ken Silva
CIO, VeriSign and
ISAlliance Chairman

Table of Contents

Introduction

Contracting for Information Security in Commercial Transactions—An Introductory Guide represents a significant new step for the Internet Security Alliance in striving to advance the quality of security on the Internet through non-regulatory, private sector solutions. This publication is the first product along that new path—an introductory guide to the architecture, vocabulary and contract structures through which information security is accomplished and strengthened across modern commercial relationships.

The security challenges facing large corporations and their business partners are complex and difficult to address:

- Companies must develop and maintain the security of their information assets within a globally competitive environment that often places two different business values into conflict – the need for strong corporate security and the value of achieving cost-effective services, particularly involving the processing and management of electronic information.

- When electronic data is involved, virtually every business is both receiving and transmitting information. As a result, the rules of engagement involving information security are often different than in many other business relationships. Information security procedures must be uniform, must be consistent and must generally work equally for all parties involved in a transaction.

- The consequences of information security incidents have become the topics of headlines in the news; as a result, companies must take closer account of their risk exposure in this area, with a greater awareness that those issues may become important at some future date.

- Government regulation of business information systems is being extended to include attention to the terms and conditions of the agreements and contracts under which data processing and other critical services are delivered. Scrutiny is being given to issues involving the security of personal information, but also complex subjects such as authentication controls, risk transfer, records archiving, forensic imaging and the security of mobile devices.

- Information security attacks have become more sophisticated. New strategies and tactics by the malicious actors continue to test the integrity of corporate information systems with increasing momentum and complexity. Companies dependent on data processing services must be capable of waging collaborative defenses with their business partners and information sources to protect the ongoing functional capability of their networks and services, discharge fiduciary obligations, and remain competitive.

In this environment, the Internet Security Alliance recognizes that the contracts by which companies – large and small – establish and manage their data processing activities with other businesses are a vital tool in the overall process of achieving effective information security in global commerce. These agreements can involve the payment of significant service fees and often involve the processing of enormous volumes of transactions, often including highly valued electronic information assets.

However, very few resources exist that help companies – including their IT professionals, information security officers, auditors and attorneys – understand how to structure the relevant contract provisions. Fewer resources exist that provide functional examples of the terms and conditions needed to express properly in commercial agreements the requirements for achieving and maintaining information security as an integral part of the relationship being established by those agreements.

As part of the mission of the Internet Security Alliance, the members commissioned and undertook to participate in the Model Contract Project – an ongoing program through which Alliance members will work to:

- better define the challenges of contracting for information security;
- promote non-regulatory solutions to problems shared throughout the business community; and
- provide contracting tools and resources that complement the ongoing dynamic evolution of technology defenses and strategies.

While there is a strong tradition in the work of the Internet Security Alliance to focus on the needs of small businesses and individuals, there was a realization that larger companies are also challenged to develop the relevant agreements and contract language. Members determined that focusing on the needs of larger companies within the Model Contract Project would achieve the added benefit of informing smaller businesses of how larger companies view the issues – it is toward that dual goal that this Guide has been developed. Unfortunately, there are no "simple" solutions to information security; the risks all companies face each day require consistent, rigorous attention for the related information assets to be protected.

Early in the Model Contract Project, participating ISA members confirmed that contracting for information security demands significant technology competency, strong awareness of the varied regulatory environments, and professional teams within companies that can communicate effectively across professional disciplines. The members uniformly agreed that one of their greatest challenges was having a starting point from which to discuss information security controls effectively with their teams and their business partners – that shared observation drove the formulation of Contracting for Information Security in Commercial Transactions—An Introductory Guide.

This Guide is intended to provide a starting point for professionals asked to develop and negotiate terms and conditions addressing information security in sophisticated commercial business relationships. While a variety of approaches were considered, the participating ISA members determined the best first product was to provide three important building blocks:

- *An Overview*—The Overview introduces the range of topics to be considered in drafting information security terms and conditions in a commercial agreement. Information security is a professional discipline requiring significant training and, for some, certification in specific fields. While the Overview is not intended to provide a summary of the entire field of information security, the Overview offers an expression of the range of topics (and their complexity) that contracts tackling information security should consider.

  While not every topic contained in the Overview will be specifically relevant in every agreement, nearly all of the topics are worth considering as companies evaluate information security concerns and structure their commercial relationships accordingly. Each company's experience will also yield understanding of additional topics requiring attention based on the nature of the data, the kind of commercial relationship envisioned and the overall value and importance of the related services.

Those familiar with information security will recognize that many of the Overview topics are also topics referenced in prevailing standards addressing information security, such as BS7799 or ISO17799. While the omission of other topics is not intended to suggest they are not relevant, the ISA members felt the topics referenced are the most important to commercial contractual relationships.

- *Glossary of Defined Terms*—Robust commercial agreements are characterized by detailed definitions of specific terms used within the agreements. Information security is like any other important subject within a contract – meanings matter, particular when the terms are highly technical in nature. The Glossary delivers a set of tools from which to proceed – the defined terms are the building blocks from which the remaining substantive terms can be addressed.

  The defined terms included in the Glossary are associated with many, but not all, of the topics included in the Overview. The definitions illustrate, by example, the challenge of migrating technical terms and concepts into contractually functional language. Taken together, the defined terms provide a vocabulary with which the more detailed and substantive terms and conditions can be constructed.

- *Model Terms for Privacy Management*—The final component of this Guide is a representative set of contractual terms under which a company that collects and *processes* personal information might regulate the management and use of that information by a service provider. While future work of the ISA Model Contract Project may address other substantive areas, the strong public awareness of the need for protecting personal information made this topic a priority to consider.

  The Model Terms have evolved out of a series of commercial transactions and represent the efforts of considerable negotiations. While intended only as an example set of provisions – addressing many topics from the Overview and using definitions set forth in the Glossary, the Model Terms help illustrate what is required for practical information security controls to be implemented in a commercial agreement.

Finally, in support of the preceding “building blocks,” this Guide includes an Annex of Selected Information Security Resources. The Annex lists various resources available on the Internet to which executives, managers and their lawyers can refer to gain further information regarding information security, applicable regulations and related topics.

As readers review and use this Guide, the following cautionary observations should be noted:

- Readers of this publication should expect to be knowledgeable of general information security principles. This Guide is not intended to provide an education in information security. The Annex of Selected Information Security Resources identifies a range of publications and services from which that education can be obtained.
- This Guide is not intended to provide a description of the statutes, regulations and other legal obligations imposed on companies relating to information security. This publication is a practical guide, intended to support and stimulate more in-depth attention to the topics considered. At all times, readers are encouraged to consult legal counsel to assist in understanding the applicable legal requirements involving information security for their specific operations.
- In all respects, this Guide is provided solely for informational purposes and does not contain or convey legal advice. The information in this Guide should not be used or relied upon with regard to any particular facts or circumstances without first consulting a lawyer.

****

The Internet Security Alliance considers the Model Contract Project to be a continuing work in progress. The Alliance welcomes comments and criticism of this Guide and hopes that this publication will encourage greater dialogue on how to better address information security within commercial relationships. Comments can be directed to modelcomments@isalliance.org.

Businesses of all sizes are encouraged to consider joining the Internet Security Alliance and becoming directly involved in our work, including the future activity of the Model Contract Project. The Internet Security Alliance (ISAlliance) is a non-profit collaboration between the Electronic Industries Alliance (EIA) and Carnegie Mellon University's CyLab and works closely with the CERT Coordination Center (CERT/CC), a leading, recognized center of Internet security expertise. ISAlliance's mission is to use the collective experience of its member corporations to promote sound information security practices, policies, and technologies that enhance the security of the Internet and global information systems.

ISAlliance members receive an array of technical, legal, business, and public policy services designed to help them protect their corporate brand and assets and comply with perpetually changing legal and industry standards and practices.

For more information about ISAlliance membership, please visit our website:
www.isalliance.org or call Jennifer Johnson, Director of Marketing and
Finance at: 703-907-7708.

Part I

An Overview of Information Security Contracting Topics

Introduction

Information security is challenging to develop and implement. When information security must be extended to assure the integrity of electronic information being transmitted to and received and processed by third parties, businesses are often surprised by the complexity of topics that must be considered in preparing appropriately protective contractual provisions. Many of these topics will introduce management demands, pricing considerations and allocations of risk and liability that are overlooked in the initial discussions between the parties.

The unexpected dimensions of structuring and managing information security will confront parties at different points in the contracting process and relationship – during initial planning, after the formulation of a letter of intent or, far too often, in the latter stages of negotiation when internal audit, information security or legal departments identify the information security issues for the first time. The impacts can be substantial – altering transition plans, management teams, economic models and, ultimately, the viability of the transaction itself.

Regarding the structure of this Overview of Information Security Contracting Topics, one of the realities of information security management is that each topic is often inter-dependent with several others. A further reality is that it is not possible to fully account for all of the information security topics relevant to commercial data processing and agreements – the field is remarkably dynamic and each cycle of time brings new technologies, new controls and new vulnerabilities to be evaluated.

As a result, the topics have simply been organized alphabetically. For each major topic, a brief description of the scope of that topic is provided and, when considered useful, representative sub-topics are included to illustrate the range of factors to be taken into account. Those topics that can be particularly complex are highlighted. In addition, the footnotes reference some of the Defined Terms that are included in Part II—Glossary of Defined Terms relevant to each topic.

Those unfamiliar with information security principles and management practices are encouraged to consult trained and experienced information security professionals, auditors and legal counsel to understand more fully the scope and complexity of the topics set forth in this Overview. In addition, many of the resources identified in the Annex of Selected Information Security Resources provide invaluable guidance.

How to Use the Overview of Information Security Contracting Topics

This Overview is primarily intended to foster dialogue and discussion. Each topic has potential applicability to a wide variety of transactions and relationships – the listings should encourage analyses by various different combinations of the stakeholders in specific transactions:

- *Internal corporate teams*—business managers, information security officers, internal auditors and attorneys can discuss how these topics impact potential functions and services for which information security controls may be appropriate. The dialogue can also be used to focus on variables that could impact – or potentially disrupt – the business case for the transaction under consideration: staffing, system infrastructure (computers, applications, security controls), regulatory exposure, funding requirements and allocations of liability.

- *Negotiation teams*—the business teams directly negotiating the related contracts or agreements can use the Overview topics for similar dialogue. As noted earlier, many of these topics are not properly addressed early in the life cycle of structuring and drafting the related agreements. This list (and similar materials, such as those identified in the Annex of Selected Information Security Resources) can stimulate an attention to those topics.

- *Attorneys*—attorneys responsible for drafting and negotiating the information security provisions of the related commercial agreements can employ the Overview to help structure and audit their own due diligence efforts to determine the scope of the contract and the terms and conditions that will be appropriate. In addition, the Overview, which has been prepared without regard to specific statutes or regulations, helps focus counsel on the practical elements that must be considered in order to implement “reasonable” and “suitable” information security controls in commercial contractual relationships.

An Overview of Information Security Contracting Topics

The following topics, arranged in alphabetical order, illustrate the range of subjects that are addressed in structuring information security controls in commercial agreements. For each topic, a brief description of the scope of the topic is provided and, when appropriate, sub-topics are identified. Note: Topics marked with an asterisk (*) are particularly complex in practice and the listings of subtopics may be insufficient without detailed internal discussions.

Account Authorization and Administration

Scope: describe controls established for authorizing and administering accounts and identities, particularly when third parties are providing such services, where the control is required to secure identified information assets or applications (such as personal information, financial data, etc.).

Applications

Scope: describe controls relating to software development activities, including the listed sub-topics, where the software may be the target of information security concerns:

- Application installation and deployment
- Application packaging
- Application testing and verification

Business Continuity Plans

(see also Incident Reporting and Response below)

Scope: describe requirements for business continuity plans, including specifically terms addressing the implementation of information security controls during any transition to contingent or back-up facilities.

Certifications

Scope: describe requirements for obtaining and maintaining certifications on information security controls, facilities, and resources maintained by the parties and related to the underlying data services being provided (such asBS7799, Common Criteria, etc.).

Change Control Policies (and Costs)

Scope: describe procedural controls (and cost allocation arrangements) for implementing change controls that may impact the operation or integrity of information security controls that have been established, with attention to each of the designated sub-topics.

- Software
- Hardware
- Services

Device Security

Scope: describe information security controls required to be employed in connection with the use of any mobile computing or communication devices (laptops, PDA's, cell phones, etc.) on which services may be performed or to or from which data may be communicated.

Employee Monitoring

Scope: describe controls imposed on the manner in which a service provider may monitor or collect information on the Client's employees (for example, the employee use of selected services or activities).

Encryption

Scope: describe controls to be required for using encryption, including controls for assuring key availability to assure access to Client records within a provider's encrypted control.

Equipment Disposal

Scope: describe requirements for the disposal of computer equipment, taking account of legal requirements in both the privacy/security and environmental control areas.

Facilities (Physical Security)

Scope: specify ranges of criteria, requirements and controls for physical security of facilities in which processing services are occurring, including review and certification:

- Design requirements
- Periodic environmental reviews
- Logical and physical access controls

Human Resources

Scope: describe requirements involving controls of Supplier personnel:

- Segregation/identification of supplier personnel
- Background checks (direct employment and subcontractors)
- Client control of Supplier personnel present at client facilities

*Incident Reporting and Response**

Scope: describe requirements for Supplier incident reporting (particularly with respect to incidents affecting systems but not specific Client data):

- Reporting of incidents on Supplier systems
- Expedited dispute resolution
- Interfaces to Client incident reporting systems

Information Security Audits

Scope: describe requirements for the auditing of information security controls and their effectiveness. These requirements may include periodic reporting, third-party audits (such as those required under SAS 70), mediation and correction programs and the like.

Insurance; Allocation of Risk

Scope: describe specific insurance coverage provisions (scope of coverage, limits, etc.) as well as other provisions allocating risks arising from security incidents (costs of notice, investigation, etc.).

Malicious Incidents/Software Management

Scope: describe responsibilities for reporting incidents, installing patches, etc., regarding trojans, spyware, worms, phishing, spam, etc.

*Network Architecture**

Scope: describe process for establishing the requirements for network architecture, implementing those requirements and managing them:

- Firewall configuration
- Network separation
- Traffic filtering
- Monitoring ports
- Threat and vulnerability

Outsourced Services—Additional Security Controls

Scope: describe requirements for managing security controls around specific functions:

- Password resets
- Security incident reporting
- Integration of ticket functions
- Accessibility of customer information

Password Management

Scope: describe controls for password management relating to Supplier employees:

- Access management
- Employee transition procedures
- Spot-checking procedures

Patch Management

Scope: describe management controls for installing and updating patches, notably those remedying software vulnerabilities:

- Timing
- Responsibility for application
- Allocation of duty based on service relationship (internal or outsourced)

Policy Controls (including Supplier-Client policy conflicts)

Scope: describe how to manage reconciliation of Supplier and Client policies.

Record Retention

Scope: describe requirements for records retention services by Supplier relating to security controls (particularly those relevant to “internal controls”) of Client (logs, audit trails, incident reports).

*Regulatory Compliance of Services**

Scope: describe specific controls imposed on Suppliers in possession of personal information assets:

- Use and disclosure of personal information
- Contractual assurances for cross-border/EU transfers

Subcontractors

Scope: describe requirements for contracts between Supplier and its subcontractors, particularly those relating to employee approval, security controls, confidentiality, etc.

Supplier Confirmation of Network and System Configuration

Scope: Describe requirements for Supplier management of configurations, including scanning of configurations, periodic intervals, and remediation.

Supplier Employee Issues

Scope: describe requirements addressing controls on Supplier employees:

- Background checks
- Client control on Client premises
- Physical identification of Supplier employees
- Privilege and function levels
- Temporary personnel
- Training (including Client policies)
- Transitioned personnel

Supplier Security Policies

Scope: describe how Supplier security policies are validated, and the manner in which the policies are to be updated and maintained based on changing security dynamics and regulations:

- Validation methods
- Maintenance and update duties

Systems Integration

Scope: describe requirements for how to integrate Supplier employee use of Client systems (focusing on management, not operational, details):

- Use of Client mail accounts

- Internet access for Supplier employees
- Use of other mail accounts

In addition to the preceding topics, the following topics are related subjects, but several of these topics could be, and often are, addressed by provisions with more comprehensive coverage than merely focusing on information security controls:

- Asset inventory and tracking
- Codes of conduct
- Migration testing and verification
- Service level agreements

Part II

Glossary of Defined Terms

Introduction

Commercial agreements often require the parties to develop and employ a shared vocabulary. In business, and in the management of information security, defined terms serve to provide clarity and certainty. Defined terms can be employed by those responsible for drafting an agreement to better map the actions and processes required by the agreement. During the term of the contract, the defined terms serve to reduce possible conflicts and facilitate better administration of the relationships.

Structuring Defined Terms. A variety of approaches are taken to identify the shared vocabulary through which an agreement might be administered. Defined terms are generally presented in one of three forms:

- The meanings are provided within the context of a specific sentence or a specific provision of the agreement, with a capitalized definition provided in parentheses:

  Example: *Client shall identify each former, current and prospective client or customer of Client ("Customer").*

- The defined terms are organized in alphabetical order at the beginning of an agreement:

  Example:

  "Client" means the ABC Corporation.

  "Customer" means each former, current and prospective client or customer of Client.

- The defined terms are set forth in a separate glossary of defined terms that appears at the end of an agreement or is separate from the agreement and is incorporated by reference in the agreement and related documents. This approach is often employed when the commercial agreement documents are numerous in number and the parties wish to economically establish one location where the definitions are provided for use across all of the agreement documents.

For the purposes of this Guide, the glossary approach has been adopted.

Dependent Definitions. In most commercial agreements, several of the shared vocabulary terms are interdependent: definitions incorporate the use of other defined terms to achieve their own respective meanings. This approach can provide significant economies to the drafting, negotiation and administration of the agreement.

As a consequence, care must be employed to assure, as the defined terms are developed, that the meanings are properly dependent upon one another and remain sensible in each instance where the terms are relied upon in the agreement's provisions. In the Glossary of Defined Terms used in this Guide, the defined terms are heavily interdependent.

How to Use the Glossary of Defined Terms

The Sample Scenario. Any sophisticated commercial agreement providing attention to information security issues will be highly customized to the specific needs of the parties and the data services to which the agreement relates. However, many attributes of the process by which information security requirements are defined, developed and implemented are frequently similar, particularly when "high value" information assets are involved.

As a result, the defined terms included in the Glossary of Defined Terms have been developed for use in the context of a scenario that has some relevance to nearly any information security implementation across commercial services. Here are the essential elements of the scenario to which the Glossary relates (these elements also carry over to the scenario for which the Model Terms for Privacy Management in Part III are presented):

- A customer ("Client") obtains from a service provider ("Provider") data processing and related services ("Services").
- The Services require ongoing data processing and communications involving Client's and Provider's networks, applications and systems. A range of different classes of information are contemplated to be

exchanged and/or processed, including "Client Information," "Personal Information," "Employee Information" and "Aggregated Data."

- Establishing the information security controls will require the development and delivery of specific services or features ("Deliverables"), for which Client will perform acceptance testing procedures. Provider and Client will employ "Security Controls" that may require "Authentication," "Certification" and "Encryption."
- Provider, among other obligations, will be required to protect against the use of "Malicious Code" and the occurrence of "Security Incidents" and will be required to report to Client on the occurrence of "Regulatory Incidents."
- Both Provider and Client are committed to establishing effective information security controls as a part of their relationship.

Practice Tips

In using the Glossary, the Defined Terms should be considered as starting points from which to evaluate the related business and legal considerations and develop an integrated view of a shared vocabulary, whether for general strategic approaches (such as uniform terms offered by a service provider) or for a specific commercial transaction.

- *Information security professionals* should strive to adapt the defined terms to reflect relevant components of their systems and business practices. Effective implementation of information security is often challenged by the practical requirement that a company not familiar with partnering with service providers must first define its own policies in sufficient detail that those policies can then be expressed to its service providers as binding obligations. The Defined Terms are an important starting point in that process.

  For example, "Policies," "Security Controls" and "Controlling Rules" each anticipate the existence of potentially significant policy architectures in place as a predicate to the implementation of information security services.

- *Business executives* may employ the defined terms to focus discussion on the management functions between the Client and Provider required to develop and implement the information security elements of the relationship. Many of the Defined Terms describe or reference business processes that should be reviewed in order to understand, among other matters, their suitability and their economic implications for the parties.

  For example, a particular transaction may not require the need for "Authentication," "Access Controls" or "Control Information."

- *Attorneys* may use the Defined Terms for adaptation to meet specific regulatory, transactional or industry requirements. Many of the defined terms will be familiar to attorneys who have structured other types of development or service agreements, though applied to the different business issues of information security.

  For example, information security requirements in financial services transactions involving personal information may be very different from the security controls applicable to the transmission and processing of sensitive health information (such as in connection with payments for medical services).

Glossary of Defined Terms

As used in the agreement(s) into which this Glossary of Defined Terms is(are) incorporated, the following terms have the following meanings:

> "Acceptance" means the affirmative written confirmation by Client to Provider that Client has determined that a Deliverable satisfies the criteria set forth or referred to in this Agreement.
>
> "Access" means (a) actual access to any Protected Information, System, Network, Equipment, Facility, Resource, Deliverable, Service or Licensed Material, or to any other property or assets of Provider or Client, whether by physical presence or by any electronic means and (b), with respect to any Protected Information, reading, writing, modifying, deleting, transmitting, transferring, communicating or intercepting the Protected Information, whether or not any of the foregoing has been authorized, directly or indirectly, by Provider or Client, as the case may be, or any entity or person acting on Provider's or Client's behalf, as the case may be.
>
> "Access Controls" means controls established for managing Access, including Passwords and other Authentication Services.
>
> "Affiliate" means, with respect to each party, any other Entity directly or indirectly controlling or controlled by or under direct or indirect common control with such party. For purposes of this definition, "control," "controlling" and "controlled" mean, with respect to each Entity, (a) the legal, beneficial or equitable ownership, directly or indirectly, of fifty percent (50%) or more of the capital stock (or other ownership interest, if not a corporation) of the Entity ordinarily having voting rights, or (b) the right or power, directly or indirectly and whether by ownership of voting securities, by agreement, or otherwise, to (i) elect a majority of the board of directors or other management of the Entity or (ii) control or direct, or cause to be controlled or directed, the management or policies of the Entity.
>
> "Aggregated Data" means and includes all Information, whether or not considered to be Information, that is created, processed, transmitted or stored by either party, that represents any of the following (a) data regarding the performance of the Obligations or any other aspect of the performance or

function of Provider under this Agreement; (b) any information representing event-level reports regarding particular transactions, events or other circumstances relating to the performance of the Obligations; or (c) any database, record or other compilation of any Information that is derived, combined, extracted, accumulated or otherwise developed in reliance upon such Information; and includes any specific records that have been created through the redaction, editing or other removal of any Information.

"Agreement" means (a) this [full title of agreement], (b) all exhibits, schedules and attachments to this [full title], (c) all Orders and Change Orders executed by the parties, (d) all amendments to any of the foregoing that are executed by the parties and (e) all other documents and instruments the parties agree in writing to include and incorporate as part of this Agreement.

"Applicable Law" means any law, statute, rule, regulation, policy or order of any governmental authority (and its instrumentalities and political subdivisions, including all states, provinces, territories and the like) within the United States and any other jurisdiction designated in this Agreement, as currently in effect or adopted or modified at a later date.

"Application" means the executable software that is part of or used in any Services, Deliverables or Licensed Materials to be provided by Provider under this Agreement, together with all related Documentation.

"Authentication" means corroboration that an Entity is who or what the Entity claims to be.

"Certification" means any certification provided by any third party relating to an Entity or any Resources (including, for example, any Systems, Networks or Applications) that is intended to evidence the compliance of the Entity or the Resources with specified Standards or SLAs.

"Change Order" means any written amendment to an Order prepared pursuant to this Agreement and properly signed by Client and Provider, numbered in the sequence in which each Change Order becomes effective.

"Client" has the meaning set forth in the preamble to this Agreement.

“Client Information” means (a) all Information furnished or made available directly or indirectly to Provider by Client or any of its Affiliates and (b) all Information about or regarding Client received or obtained by Provider from any other Entity.

“Code” means any and all Source Code, object code, programming code, binary code, algorithms, development tools, graphical interfaces, media conveyors, embedded software, standardized subroutines, command structures, processes, menus, navigational aids, programming techniques, scripts, software language and message formats used by a software application program to communicate with or to transfer data or information between software applications or programs (such as, but not limited to, application program interfaces), or other similar codes (including, without limitation, HTML, XML or similar codes), methods or processes related to computer programming, whether or not deployed over the Internet as a web site, and all Documentation relating to the foregoing, together with all Intellectual Property and other rights relating to the foregoing. “Code” includes all translations of any Code into any different programming languages.

“Confidential Information” means any and all proprietary, non-public or confidential Information provided or disclosed by or on behalf of one party to the other party, or obtained in any other way by one party about or relating to the other party, including all Protected Information, Code, Records, Customer lists, Intellectual Property, processes and the terms of this Agreement, regardless whether the party providing such Information designates, labels or otherwise identifies it as “confidential” or “proprietary” or with some other similar appellation.

“Configuration” means any configuration, design or similar Record developed and used in the administration of any Systems.

“Control Information” means any Information used for Access and other control purposes.

“Controlling Rules” means any Applicable Law and Client’s Policies.

"Customer" means each former, current and prospective client or customer of Client.

"Customer Information" means all Information delivered, disclosed or otherwise made available to or obtained by Provider by, on behalf of or from Client or any of its Affiliates that, alone or in combination with other Information held or accessible by Provider, uniquely identifies any Customer. "Customer Information" includes any copies of such Information, or any derivations, combinations, extractions, accumulations or other aggregations of such Information, which continue to permit such unique identification to be made.

"Data" means all Client Information in electronic or hardcopy form that is collected, processed, entered, stored, maintained or otherwise transmitted or used in any way by Provider in, or in connection with, its performance of the Obligations.

"Deliverable" means all Intellectual Property, all other tangible and intangible property, and all other items and materials, including related Documentation, that are to be provided by Provider to Client under this Agreement and that Client will own, and any and all Work Product related to any or all of the foregoing.

"Design Materials" means and includes (a) any and all of Client's requirements and Provider's specifications for the Applications, Services, Deliverables and Licensed Materials, all as set forth or referred to in this Agreement, and all other documents mutually designated as part of the Design Materials, together with (b) all other Records created, developed, received or obtained by Provider and accepted by Client that describe the intended functionality, design, architecture or performance requirements of Applications, Services, Deliverables or Licensed Materials.

"Desktop Environment" means Client's desktop environment which consists of desktop computer Equipment, desktop computer software, and any cabling among the desktop computer Equipment or between the desktop computer Equipment and the wall jack.

“Device” means any computer, server, laptop computer, peripheral, hand-held, mobile or other device that is employed on, or connects to, any Network or System.

“Disaster” means any unplanned event or condition (including a Force Majeure Event) that causes (a) any Facility to be inaccessible or inoperable, (b) any Equipment used or employed by Provider or any other Entity in any way in, or in connection with, the performance of the Obligations to malfunction or be inoperable or (c) the performance of any Obligation to be impossible or commercially impracticable.

“Documentation” means all of the following, whether in tangible or electronic form: user manuals, help guides, user support materials, reference text, design schematics, developer documentation, training tools and materials, all Records and materials comparable to any of the foregoing, and all modifications of any of the foregoing.

“Employee Information” means all Information delivered, disclosed or otherwise made available under or in connection with the performance of this Agreement to Provider by or on behalf of Client or any of its Affiliates that, alone or in combination with other Information held or accessible by Provider, uniquely identifies a current, former or prospective Staff Member of Client or any of its Affiliates. “Employee Information” includes any copies of such Information, or any derivations, combinations, extractions, accumulations or other aggregations, from which such unique identification can be made.

“Encryption” means the use of an algorithmic process that transforms data or a message (the “plaintext”) into another form (the “ciphertext”) such that (a) the plaintext can be recovered from the ciphertext by a person or algorithm possessing a certain value (the “decryption key”) and (b) recovering the plaintext from the ciphertext is difficult to infeasible by any agent not in possession of the decryption key.

“End User” means (a) each of Client’s Staff Members and Customers that receives or has Access to the Services and (b) all other Entities identified by Client to Provider as End Users.

"Entity" means any individual, corporation (including, any for-profit or non-profit corporation), general or limited partnership, limited liability company, limited liability partnership, joint venture, estate, trust, business trust, association, organization, governmental body or agency or other entity.

"Equipment" means all computer and telecommunications equipment (without regard to the entity owning or leasing such equipment) and associated peripherals and cables, and includes: (a) computer and server equipment, including associated attachments, features, accessories, cables, printers and other peripheral devices; and (b) telecommunication equipment, including voice response units, automatic call distributors, multiplexers, CSUs/DSUs, hubs, bridges, routers, switches and associated cables and wires.

"Error" means any error in any Application, Service, Deliverable or Licensed Material that prevents the Application, Service, Deliverable or Licensed Material from operating or being provided in accordance with (a) the applicable Design Materials and (b) any other applicable criteria, requirements, Specifications or Standards set forth or referred to in this Agreement.

"Facility" means each building or other physical facility owned, rented, occupied, accessed, visited or used in any way by Provider in, or in connection with, the performance of the Obligations, including Client's facilities and all third-party facilities that house any Equipment or Resources used or employed by Provider or any other Entity in any way in, or in connection with, the performance of the Obligations.

"Force Majeure Event" means fire, flood, earthquake, elements of nature, acts of God, riots, civil disorders, acts of war, acts of terrorism, or any other event beyond the reasonable control of a party, but excluding events caused by or resulting from the actions or omissions of, or from the failure to perform or fulfill contractual obligations by, a third party with which the party to this Agreement, or any of its Affiliates, has a contractual relationship.

"Information" means (a) all information, data, content, knowledge, intelligence, facts, concepts, ideas, plans, materials, disclosures, statements, communications, instructions, representations, signals, characters, numbers, texts, records, documents and instruments, in any form or format and on or through any medium, and (b) all copies, summaries, abstracts, indices, outlines, reports, compilations, derivations, combinations, extractions, accumulations, aggregations, tables of contents and other representations or embodiments of any kind of all or any part of the foregoing.

“Intellectual Property” means all (a) patents, patent applications, patent disclosures and inventions (whether patentable or not), (b) trademarks, service marks, trade dress, trade names, logos, corporate names, Internet domain names, and registrations and applications for the registration thereof together with all of the goodwill associated therewith, (c) copyrights and copyrightable works (including mask works) and registrations and applications thereof, (d) Code, Data, databases and Documentation thereof, (e) trade secrets and other confidential or proprietary information (including ideas, formulas, compositions, inventions, improvements, know-how, manufacturing and production processes and techniques, research and development information, drawings, specifications, blueprints, flowcharts, schematics, protocols, programmer notes, designs, design rights, developments, discoveries, plans, business plans, proposals, technical data, financial and marketing plans and Customer and Supplier lists and information), (f) waivable or assignable rights of publicity, (g) waivable or assignable moral rights, (h) all other forms of intellectual property and (i) copies and tangible embodiments of any or all of the foregoing (in whatever form or medium).

“Internet” means the interconnected system of Networks that connects computers around the world via the TCP/IP protocol.

“Licensed Materials” means all Intellectual Property, all other tangible and intangible property, and all other items and materials for which a license is granted or to be granted by Provider to Client pursuant to this Agreement. “Licensed Materials” includes all Documentation related to any of the foregoing.

“Maintenance Services” means all Services to be performed by Provider, as described in more detail in [the Maintenance Services Agreement between the parties], to maintain and support Deliverables and Licensed Materials.

“Malicious Code” means and includes any virus, trojan horse, worm, malware, Self-Help Code or other software programs, instructions, designs or routines or hardware components designed to permit, or that do permit, unauthorized access to or use of all or any part of any Data, Application, Deliverable, System, Network or any other Resources of Client, or that (a) function to disable, erase, harm, or render inoperable or otherwise incapable of being used in the full manner for which they were designed and created, all or any part of any Data, Application, Deliverable, System, Network or any other Resources of Client, (b) replicate, transmit or activate themselves without the control of an Entity operating a System on which any such program resides, (c) contain any key, node lock, time-out or other function that is not disclosed in the related Documentation that restricts or may restrict use of or access to any Application, or (d) facilitate the performance or effect of any of the foregoing.

“Network” means a system of interconnected Equipment or Systems, and includes the Code necessary for the proper functioning of the foregoing.

“Obligations” means any and all of Provider’s duties, obligations and responsibilities under this Agreement.

“Open Source Code” means: (a) any Code that requires, as a condition for the use, modification or distribution of such Code, that such Code comply with the Open Source Software Requirements or (b) any Code that contains, is derived in any manner (in whole or in part) from, or statically or dynamically links with any Code specified in the preceding clause (a). For the purposes of this definition, “Open Source Software Requirements” means the Code: (c) must be disclosed or distributed in source code form; (d) must be licensed for the purpose of making derivative works; or (e) can be redistributed only in a manner that does not permit any Person to claim enforceable rights in any Intellectual Property. By means of example only and without limitation, any Code licensed or distributed under any of the following licenses or distribution models will be deemed Open Source Code: (u) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (v) the Artistic License; (w) the Mozilla Public License; (x) the Common Public License; (y) the Sun Community Source License (SCSL); or (z) the Sun Industry Standards Source License (SISSL).

“Order” means each written order prepared and executed by Client and Provider, substantially in the form of Exhibit ___ and as amended by all applicable Change Orders, that contains a description of Services to be provided or other Obligations to be performed by Provider.

“Password” means a string of characters used to gain Access.

“Personal Information” means all Information related to specific individuals that, collectively or in part, directly or indirectly identifies such individuals. “Personal Information” shall include, but shall not be limited to, all: (a) “nonpublic personal information,” as defined by applicable regulations implementing the U.S. Gramm-Leach-Bliley Act found in Regulation S-P (17 C.F.R. Part 248), (b) all “consumer reports,” as defined by the U.S. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681a(d), (c) all “protected health information,” as defined by applicable regulations implementing the U.S. Health Insurance Portability and Accountability Act (HIPAA) found at 45 C.F.R. § 164.501, (d) all other similar information identified by Client as Personal Information, and (e) any similar categories of information identified in any Applicable Laws.

“Policies” means, with respect to any Entity, any and all policies, controls and guidelines established by the Entity to govern operations, internal controls, contractor relations, physical security, the security of Networks or Information Systems, the privacy of Personal Information, the management of Records, the execution of Security Controls, and other matters relating to the Entity’s business or affairs.

“Protected Information” means, collectively, all Data, all Client Information, all Employee Information, all Customer Information and all Control Information.

“Provider” has the meaning set forth in the preamble to this Agreement. Unless the context requires otherwise, “Provider” includes all of Provider’s Staff Members and all Subcontractors (and their Staff Members) that perform any of the Obligations or provide any of the Services.

“Record” means any and all information that is inscribed on a tangible medium or stored in an electronic or other medium and is retrievable in perceivable form, whether presented as graphics, text, audio or video, or in any other format.

“Regulator” means each federal, state and local governmental Entity with regulatory authority or jurisdiction over or with respect to Client, Provider, the activities or operations of either of them, the Obligations, the Services, or any other activities or transactions contemplated under this Agreement.

“Regulatory Incident” means the potential or actual violation of any Applicable Law arising from, in connection with or related to the performance of the Obligations or the provision of the Services.

“Resources” means, with respect to either party, all resources employed or needed by the party to perform its respective obligations under this Agreement, and in the case of Client, to use, receive and benefit from the performance of the Obligations.

“Security Breach” means a confirmed loss of, or unauthorized Access to, any Information, System, Network, Resource or Facility, including incidents involving the unauthorized physical penetration of any Facility.

“Security Controls” means all of the controls and procedures, whether pursuant to this Agreement, Controlling Rules, reasonable commercial practice or otherwise, to be employed and followed by Provider in connection with the performance of the Obligations and provision of the Services and the operation and use of Provider’s Resources in the performance of the Obligations and provision of the Services to ensure the security and integrity of all Information provided to or received or obtained by Provider. Security Controls may include those controls or procedures that are intended to (a) ensure the physical security of any Resources used to perform the Obligations and provide the Services, (b) protect the integrity of all Protected Information against improper or negligent access, loss, alteration, destruction, interception or compromise, whether during the performance of the Obligations or provision of the Services or in the use by Client or any Entity of any Protected Information, (c) provide Authentication regarding the sender of any communication or user of any Code or System or (d) protect the integrity and accuracy of, and detect errors in, the transmission or content of any communication or Records. A Security Control may require, among other techniques, the use of algorithms or other codes, identifying words or numbers, Encryption, callback procedures or other control, Authentication and security procedures, devices and methodologies.

“Security Control Updates” means any change to any Security Controls, whether required by Client or by changes in any Controlling Rules or initiated otherwise by Provider.

“Security Incident” means the potential loss of, or an attempted or potential unauthorized Access to, any Information, System, Network, Resource or Facility, including incidents involving the potential physical penetration of Facilities.

“Self-Help Code” means and includes any back door, time bomb, drop dead device, or other software design, instruction or routine designed to disable, or otherwise capable of disabling or rendering inoperable or impairing the operation of, in whole or in part, a computer program automatically with the passage of time or under the positive control of Provider or any Entity other than Client. “Self-Help Code” does not include any devices or software routines in a computer program, if any, designed to permit Client (or any other Entity, other than Provider, acting on behalf of Client) to obtain access to any Application or Deliverable (e.g., by remote access by modem) for purposes of performing maintenance services.

“Service Level Agreement” or “SLA” means any requirements for functional services or activities that are capable of being measured, as expressed in the SLAs or any other Documentation.

“Service Provider” means any Entity, other than Provider and Subcontractors, that provides any goods or services to Client [or to Provider].

“Services” means any and all services Provider is to perform for Client under this Agreement, including installation, integration, customization, development, training, support, consulting and Systems analysis services, and Maintenance Services, as described in further detail in this Agreement.

“Source Code” means and includes, with respect to each Application, all of the programming statements and instructions constituting part of any Code or

Open Source Code, together with all compilers, assemblers and other interpreters, whether owned by Client or Provider or licensed from any other Entity, used to compile the related object Code for the Application.

“Specifications” means the requirements set forth or referred to in this Agreement for Deliverables, Services and Licensed Materials.

“Staff Member” means, with respect to each Entity, each employee, contractor, consultant, temporary worker or other person retained, employed, hired, engaged, used or paid by such Entity.

“Subcontractor” means each Entity, other than an employee of Provider, that (a) Provider engages or intends to engage to perform any of the Obligations or provide any of the Services, or (b) performs any of the Obligations or provides any of the Services, whether or not authorized by Provider to perform such Obligations or provide such Services and whether or not such performance or provision was approved at any time by Client.

“Supplier” has the meaning set forth in the preamble to this Agreement.

“System” means any combination of Equipment, Code, software, Data and other networking or communications infrastructure with, by or on which any Application or other Deliverable is developed, modified, tested, installed, run or used, or is to be tested, installed, run or used, by Client, Provider or any other Entity.

“Term” means the term of this Agreement.

“Termination” means the termination or expiration of this Agreement.

“Test Deliverable” means each Deliverable that is subject to Acceptance testing under this Agreement.

“Tools” means any tools, utilities or other devices or Applications installed or operated in connection with any Resources for the purposes of measuring one or more functional services or activities, including those services or activities subject to SLAs.

“Wireless Network” means a Network without connecting cables that relies on radio waves for transmission of data within the Network.

“Work Product” means any and all work product, Records or other materials created or developed by Provider under this Agreement, including all work in process, whether or not constituting any Deliverables or other Design Materials, regardless of the state of completeness, whether in tangible or electronic form and whether presented as graphics, text, audio or video, or in any other format.

Part III

Model Terms for Privacy Management

Introduction

For many businesses, the new legal framework governing the protection and use of personal information—the law of privacy—has been the most influential driver placing information security on the agenda of senior executives and boards of directors. But in responding to the regulatory mandates, many companies have discovered that the management practices and information security controls required to effectively manage privacy also serve as useful structures through which to help manage the security of other kinds of electronic information as well as a wide variety of transactions.

This Part III presents a robust, integrated set of Model Terms. The Model Terms address the process of developing and managing information security within the context of a more complete commercial relationship in which a Provider is performing Services for a Client. In particular, the Model Terms emphasize how information security controls might be implemented in association with the management, processing and transfer of "Personal Information." However, those studying the Model Terms will quickly realize that, with few adaptations, the potential use and applicability of the Model Terms extends far beyond transactions in which "Personal Information" is involved.

The challenge of contracting for information security in commercial transactions is reflected by the Model Terms. While an initial review might likely trigger astonishment at the number of provisions (as well as the complexity of their interdependency), those Internet Security Alliance members involved with the Model Contract Project largely confirmed that the Model Terms are consistent with contracting terms and conditions in agreements they have seen, both as Clients and as Providers. In fact, the complexity made it impracticable to develop for this Guide a full set of Model Terms for all of the information security topics that may be relevant (as represented, for example, by the Overview of Information Security Topics in Part I of this Guide).

How to use the Model Terms

The Sample Scenario. In presenting the Glossary of Defined Terms, this Guide introduced a sample scenario as a context for considering the defined terms (see page 16). For the purposes of the Model Terms, the elements of the sample scenario remain applicable and should be reviewed before studying the Model Terms. In addition, to give context to the treatment of Personal Information, the following elements are applicable to the Model Terms:

- The Client engages in the business of financial services involving operations in multiple jurisdictions; the Provider will perform the Services in those locations, as well as from additional jurisdictions in which the Client is not physically conducting business (this is a common situation where business services are being outsourced to "offshore" service providers).
- The Model Terms anticipate that Client has established specific policies and controls for information security ("Policies"); in addition, the Client's management of Personal Information is subject to various legal requirements ("Applicable Law").

Practice Tips

In using the Model Terms, like any resource relied upon for contract drafting, the language provided should be considered as starting points from which to develop terms and conditions acceptable to all of the relevant parties. As with any contract or agreement, the final version signed by the parties can evolve significantly through drafting and negotiation rounds; terms addressing information security controls are no different. The Model Terms are intended to be part of larger agreements that will contain many other relevant provisions, such as those addressing project management, performance reporting, payment of fees and expenses, allocations of liability, indemnification, termination and transition.

One very common approach to integrating information security controls into a commercial agreement is to develop the relevant terms as a separate annex or appendix, to be incorporated into the primary agreement by reference. The Model Terms have been organized to facilitate that approach; however, in different circumstances, the provisions may be more properly integrated into the body of the primary agreement.

- *Information security professionals* may employ the Model Terms to evaluate, whether as Client or Provider, the suggested duties and responsibilities. Governance of information security across connected systems is extremely difficult to manage and the Model Terms suggest only one possible arrangement of the various components. Those responsible for information security must make sure that the governance model works for their systems and operations and, if needed, recommend adaptations, additions or replacements within the Model Terms.

- *Business executives* may evaluate the Model Terms to understand additional services, fees, costs and legal exposure that may need to be considered in structuring the core economic elements of a transaction. Based on the sensitivity of the information to be protected, the sophistication of the parties, the prior experience of the parties, and ongoing regulatory dynamics, the scope of effective information security can alter the transaction. The Model Terms highlight some of those variables.

- *Attorneys* may use the Model Terms to construct appropriate commercial agreements. These provisions are not “boilerplate”; they anticipate material commitments of resources and expenditures to achieve effective information security. Attorneys working with the Model Terms should assure that, whether directly or in reliance on other team members, they possess the necessary understanding of the underlying information security practices.

Model Terms for Privacy Management

1. “Core” Information Security Provisions

1.1 Provider’s Security Obligations

1.1.1 Compliance with Security Controls and Controlling Rules

Provider shall perform the Obligations, provide the Services, and make available and apply its Resources in accordance with all applicable Security Controls and Controlling Rules. Client shall be responsible for providing to Provider a copy of any of Client’s Policies with respect to security procedures and Controlling Rules. Client shall be responsible for identifying any Applicable Laws to be considered part of the Controlling Rules that relate to any Services or Deliverables. Client will identify any such Applicable Law either in Orders or in subsequent written notices to Provider.

1.1.2 Security Policy

Prior to [the Effective Date], Provider has provided, and not less than once during each year of the Term Provider shall provide, to Client one or more briefings on the Security Controls. Client shall cooperate with Provider in receiving such briefings in a manner that protects the confidentiality of the Security Controls. However, Client shall be entitled to receive such briefings in such reasonable detail as often as Client determines to be appropriate. As part of such briefings, Provider shall permit Client to review any Audit or other similar reports that describe or assess the Security Controls relating to Provider’s performance of the Obligations and provision of the Services, and with respect to Provider’s Resources, and Client shall be entitled to assure itself that corrective actions described in such reports, if any, have been taken by Provider. Notwithstanding the immediately preceding sentence: (a) Provider shall promptly perform any corrective action recommended (i) in any reports described in such sentence or (ii) by any audit report and (b) the parties acknowledge that, among other things, the Controlling Rules may require Provider to implement Security Control Updates which, if required by Client, Provider will promptly implement upon Client’s request, provided that Provider shall not implement any Security Control Updates that are not required by Client without Client’s prior written consent, which consent shall not be unreasonably withheld.

1.1.3 Further Assurances

Provider shall execute and deliver to Client any collateral agreements Client may request relating to Provider's compliance with Security Controls and Controlling Rules, or otherwise relating to the establishment, maintenance and use of Provider's Resources for protecting the confidentiality, security and integrity of any Information obtained by, or accessible to, Provider through the performance of the Obligations, including any such agreements relating to Personal Information or as may be required by any Security Controls or Controlling Rules.

1.2 Policy Controls

1.2.1 General

In performing the Obligations and providing the Services, Provider will comply with the Controlling Rules and, to the extent not inconsistent with the Controlling Rules, the Provider's Policies. To the extent there is any conflict between the Controlling Rules and the Provider's Policies, Provider will comply with the Controlling Rules except that, in the event of a conflict between the Provider's Policies and the Client's Policies, Provider will observe the policy requirement(s) that is (are) more protective of the Client Information, as determined by Provider in good faith after consultation with Client. If, as a result of Provider having to comply with a Client's Policy where such Client's Policy is more protective of the Client Information than a Provider's Policy, Provider would suffer a material adverse impact on its performance of the Services or on its cost to perform the Services, then Provider may notify Client of such material adverse impact. In such event, Client will nonetheless have the right to require Provider to comply with such Client's Policy and the consequences of the material adverse impact to Provider of doing so will be addressed by the parties through the dispute resolution process provided for in this Agreement. Prior to the first [key date or occurrence, such as launch or delivery], the Parties will conduct a comparison of the Provider's Policies and the Client's Policies to identify any instances where the Client's Policies impose additional or different obligations on the Provider that are inconsistent with the Provider's Policies and will cooperate with each other to identify any inconsistencies or conflicts. The preceding requirements of this Section do not obligate Provider to abandon compliance with the Provider's Policies in any circumstance, other than those in which such a conflict is determined to exist. In its receipt or use of the Services, including access to Provider's Systems or Facilities, Client will comply with the

Provider's Policies, unless to do so would violate the Controlling Rules or except to the extent provided otherwise by this Agreement. Provider will, at all times during the Term, observe and implement all relevant Client's Policies with respect to any Services provided at any Client site, with respect to using the Client's Systems or the Desktop Environment, or with respect to using the Provider's Systems.

1.2.2 Conforming Provider's Policies

Subject to Section 1.2.1 above, Provider will effect any changes in its Information security practices and procedures, as conducted at any Facilities or on any Systems used to provide the Services or perform the Obligations, needed in order to implement any of the Client's Policies, except that Provider will not be required to effect any such change where its current practices are more protective of the security, privacy, and confidentiality of Information.

1.2.3 Checking Compliance

Prior to the [relevant event or date], Client will have the rights and obligations, including as provided by this Agreement, to perform audits, tests, or examinations of any aspect of the Provider's Systems, the Provider's Facilities, or any other aspect of Provider's preparations to provide the Services or perform the Obligations as reasonably necessary to verify that Provider has complied with all relevant Controlling Rules. Any such audit, test or examination will be conducted in accordance with the relevant provisions set forth in Section 2.2, and the parties will follow up on the results of any such audit, test or examination, including Provider implementing any necessary corrective or remedial action.

1.2.4 Changes to Client's Policies

Client may, from time to time in accordance with this Agreement after giving reasonable written notice to Provider, introduce new Client's Policies or delete or modify any of the Client's Policies. Such changes may include, without limitation: (a) changes initiated by Client to update security practices, Client operations, or execute other reasonable purposes not required by Applicable Law and (b) changes required by Applicable Law (including Client's interpretations of the implementation of any Applicable Law). Changes to the Services to reflect changes in Client's Policies made in accordance with this Section will be implemented by Provider in consultation with Client.

1.3 Malicious Incidents/Software Management

1.3.1 Software Transparency

With respect to all Provider-owned Applications used in the provision of the Services or the performance of the Obligations, or included in any Deliverables, Provider shall provide, as and when requested by Client, written information regarding (a) the manner in which such Applications have been designed and authored, (b) the methods used for ensuring the absence of vulnerabilities arising from negligent or willfully malicious Code preparation or processing in the creation of such Applications, (c) the quality control testing and validation controls that were employed in the creation of such Applications, and (d) the level and manner of use of, and the processes employed for detection of the presence of, Open Source Code in such Applications.

1.3.2 Open Source Code

Except as disclosed in writing to Client as part of an Order, Provider shall not (a) use or employ any Open Source Code in or in connection with the performance of any Obligations or provision of any Services, including internal development and customization activities; (b) include in any Deliverables any component or module of Open Source Code; or (c) deliver any Deliverables the use or operation of which will require the use of any Open Source Code by any System or by Client, Provider or any other Person. Provider shall, at its expense, employ software to test all its Resources and all Applications and other Deliverables for the use or inclusion of, and for reliance on a System's use of, Open Source Code, and shall certify the results of such test to Client.

1.3.3 Systems Monitoring

Provider acknowledges and agrees that Client will have the right to install compliance monitoring technologies on (a) the Client's Network connections to the Provider's Systems and (b) any Provider's Systems (other than Provider's Systems used to provide services to multiple Provider customers), that Client deems appropriate at any time during the Term, subject to the limitations of any Client's Policy and to any reasonable limitations of Provider's Policies or this Agreement, and provided that such monitoring technologies do not interfere with Provider's ability to perform the Obligations and provide the Services in accordance with the

Service Level Agreements. Where Client is prevented from installing monitoring software on any Provider's Systems because such Systems are used to provide services to multiple Provider customers, Provider shall provide monthly reports to Client concerning Client Information held or maintained on such Provider's Systems. Client and Provider shall cooperate in designing a standard form for such reports, provided that such reports will contain, at a minimum, information regarding intrusion detection events, logs, malicious code, and Data activity. Provider shall make monitoring ports available, as appropriate, to support intrusion detection events, logs, data, and other monitoring of the connection from the Provider's Networks to Client's Networks. If any monitoring technology identifies a failure in Provider's performance of the Obligations or provision of the Services to comply with Client's Policies as required in this Section, the procedures described in [dispute resolution section] will be followed.

1.3.4 <u>Source Code Escrow</u>

To protect Client's rights under this Agreement, Provider shall either (a) provide to Client a copy of all Source Code, all related Documentation and all other materials and Code necessary to maintain and use the Source Code and related Documentation (collectively, the "Copied Items") for all Applications that are included in any Deliverables or (b) keep and maintain current the Copied Items in escrow (the "Escrowed Items"). All Escrowed Items shall be escrowed with a commercial escrow agent acceptable to Client, pursuant to an escrow agreement by and among Provider, Client and such agent. Such agreement shall authorize the escrow agent to release the Escrowed Items to Client if and when Client shall have a right thereto pursuant to that agreement or this Agreement, or if Provider fails to maintain the escrow as provided in this Section. In the event of any conflict between the terms of any such escrow agreement and this Agreement, the terms of this Agreement shall govern. Provider shall pay all costs of establishing and maintaining the escrow of the Escrowed Items, including the fees of the escrow agent. Client shall have the right at any time to verify that the copy of the Escrowed Items exists in the escrow and is maintained on machine readable media compatible with Client's Systems. When any modification or other change is made to any of the Escrowed Items by or on behalf of Provider during the Term, a copy of the modified or changed Escrowed Items that includes the modification or change shall be delivered to the escrow agent not later than 5 business days after the modification or change is effected by or on behalf of Provider. Provider shall cause that a copy of the

Escrowed Items as they existed prior to the two most recent revisions after each applicable Acceptance date shall continue to be held in escrow as provided in this Section.

Provided that Client is not then in material default under this Agreement, Provider shall cooperate with Client in causing the escrow agent referred to in this Section to release the Escrowed Items to Client within five days after Provider's receipt of Client's written request, or, if applicable, Client shall have the right immediately to access and use the Copied Items, upon the occurrence of any one or more of the following events: (a) all or any material part of such Source Code is generally made available by Provider, with or without additional cost, to other users of programs similar or identical to the Applications to which the Escrowed Items correspond; (b) Provider ceases, for any reason, to do business; (c) Provider is in default under this Agreement in whole or in part because of its failure to maintain, or otherwise comply with any Obligations with respect to, such Applications; (d) sale of all or substantially all of the assets of Provider; or (e) bankruptcy, receivership, insolvency, reorganization, dissolution, liquidation, or similar proceedings are instituted by or against Provider or all or any substantial part of its property under any federal or state law.

1.4 Incident and Breach Reporting and Response

1.4.1 Incident and Breach Reporting and Investigation

Provider will comply with all Client's Policies related to the reporting of Security Incidents and Security Breaches[, including [specifically identify policies]]. Provider will report Security Incidents and Security Breaches into Client's reporting and escalation functions in the manner specified by Client or, in the absence of any specification by Client, in the same manner that similar Security Incidents and Security Breaches were reported or escalated by Client prior to the handover of the Services (or as Client may modify such procedures during the Term).

Provider will define, in conjunction with Client, a rapid response procedure and rapid response team for those Security Incidents and Security Breaches identified by the rapid response team as requiring immediate action. Provider will use commercially reasonable efforts to see that Provider's Staff Members note and report to the appropriate person within Provider: (a) any observed or suspected security weakness or Security Incident or Security Breach in the Provider's Systems, the Client's Systems, or the Desktop Environment; (b) any discovered malfunctions that cause or could cause a Security Incident, a Security Breach or a Regulatory Incident; or (c) any event-level incidents that may be indicative of larger, adverse security events (e.g., denial of service, virus penetration, etc.). Provider will promptly notify Client of all of the foregoing. Provider will also establish appropriate mechanisms, including audit trails, to identify and remedy the types, volumes and costs of such weaknesses, incidents and malfunctions. Provider will identify and implement appropriate practices and controls intended to prevent recurrence of the same.

After using commercially reasonable efforts to confirm the existence of one of the following events or situations, or as further specified by the parties, Provider will notify Client: (a) by telephone and e-mail, in either case to be confirmed in writing within one (1) business day, of any actual or perceived security risks or weaknesses detected by Provider (or notified to Provider by a third party) in the Provider's Systems, the Client's Systems or the Desktop Environment, or with respect to Provider's Staff Members or to any aspect of the Services or the Obligations; (b) of any actual or suspected breach of any Client's Policies or any Applicable Law by Provider's or Client's Staff Members, and any Security Breach or Security Incident that has affected or attempted to affect the Client Information, the Client's Systems or the Desktop Environment; and (c) of any actual evidence of involvement by Provider's or Client's Staff Members in adverse security events (e.g., password replacement, adverse remote access requests, etc.).

1.4.2 Post-Incident Actions

If Provider identifies a security risk, Provider will, to the extent possible, immediately take all appropriate steps to prevent impact to the Services, the Provider's Systems, the Client's Systems and the Desktop Environment, including all Networks associated with the provision of the Services or the performance of the Obligations, and will promptly communicate the existence of such security risk to Client. If Client becomes aware of a security risk, Client may take any action necessary to mitigate the security risk including: (a) suspending Access to any End User or Provider's Staff Member while the security risk is investigated; and (b) immediately directing Provider to conduct an investigation of such security risk believed to have originated or occurred within Provider's premises, Provider's

Systems or Provider's Networks, and promptly reporting the results of such investigation to Client.

During any period of suspended Access, Client will continue to pay amounts owed under this Agreement for Services rendered by Provider in a manner consistent with and as required by this Agreement, and Client will have the right to withhold payment of amounts for Services that were not rendered by Provider in a manner consistent with and as required by this Agreement. To the extent that Client's exercise of such right materially adversely affects Provider's performance of the Obligations, including meeting Service Level Agreements, Provider will be relieved of those Obligations for the duration of the suspended Access (except where the underlying security risk is a result of Provider's failure to perform the Obligations or provide the Services in accordance with this Agreement), provided that Provider promptly delivers written notice to Client of such impact and cooperates with Client in performing any temporary actions or services to mitigate the adverse effect upon the Services.

If, after investigation of a Security Incident or Security Breach by Client, Client reasonably determines that Provider's practices need to be amended, Provider will promptly implement any actions reasonably required by Client that are directed at preventing Security Incidents and Security Breaches from occurring again.

1.4.3 Annual Audit and Incident Report

Subject to any restrictions of this Agreement, as part of the audit process described in Sections 1.6.3 and 2.2 and to the extent not previously reported by Provider to Client, in addition to all other reporting obligations Provider has under this Agreement, Provider will provide to Client, on an annual basis (unless otherwise noted), details of the nature and severity, any effect of, and Provider's response to, the following since the beginning of the Term or the end date of the last report provided under this Section: (a) any breach of security discovered by or known to Provider that has caused, or that is believed to potentially cause, an adverse affect either on the Services, Client or Customers; (b) adverse security audit findings with respect to the provision of the Services or the performance of the Obligations; (c) any known vulnerability in Provider's Systems (or Provider software) that presents a risk to any Client Information, the Client's Systems, the Client's Networks, or the Desktop Environment; (d) any known breach of the Obligations with respect to the Client's Policies or Provider's Policies; (e) recorded or suspected

Security Incidents and Security Breaches that occurred during the audit period or were discovered during the audit process; and (f) to the extent not covered by the above, any actual or suspected breach of Information security or physical security, not previously reported, discovered by Provider to have adversely affected, or believed to have potentially an adverse effect upon, any Client Information, Client's Systems, the Desktop Environment, or Provider's Systems. Such Provider reporting procedures must be sufficient to identify, at an event level, any Security Incident or Security Breach in which Client Information was disclosed, is believed to have been disclosed, or was at risk of being disclosed, in an unauthorized manner.

1.5 Account Authorization and Administration

1.5.1 General

Provider will have responsibility for all Access Controls described in this Agreement, including account authorization and authorization for Access for Provider's Staff Members[, but Client will create such accounts and administer them]. All Access Controls and authorizations for accounts and Access by Provider's Staff Members will be conducted by Provider in accordance with the Client's Policies.

Access accounts for Provider's Staff Members must identify such individuals as Provider's Staff Members and group such individuals appropriately. All accounts to which Provider's Staff Members have or gain Access: (a) will be provisioned, maintained and terminated in accordance with all applicable Client's Policies; (b) will be kept to the minimum number necessary (both in terms of the level of each individual's Access, as well as the number of authorized users) for effective performance of the Obligations and provision of the Services; (c) will have reasonable auditing, logging, and monitoring enabled as much as possible, acknowledging that having auditing, logging and monitoring at all times may adversely impact the performance of the Provider's Systems, the Provider's Networks, the Client's Systems or the Client's Networks, and accordingly the parties will mutually agree on a procedure defining the types of auditing, logging and monitoring that will be enabled at particular times so as to reasonably meet Client's needs while minimizing adverse impact on such Systems or Networks; (d) will be deleted as soon as reasonably practicable for all Provider's Staff Members who cease providing Services for whatever reason, but in any event, no later than the end of the next business day; and (e) will be appropriately amended for those Provider's Staff Members changing responsibilities.

In no event may Provider's Staff Members share Access IDs or be provided with generic IDs. No Provider's Staff Members will be given Application level IDs, except in limited cases and only as necessary to perform the Obligations and provide the Services.

All Access accounts for Provider's Staff Members must be reconfirmed no less frequently than quarterly. No such reconfirmations may take effect until authorized by Client, which authorization will not be unreasonably withheld or delayed. All such reconfirmations must be based on: (a) continued employment of the Provider's Staff Members (with either Provider or the relevant Subcontractor), and (b) continued business need for each such individual to have the level of Access rights associated with that individual's Access account.

Access by Provider's Staff Members will cease upon Termination, except as authorized on a case-by-case basis by Client. Client will have full control over account authorization and authorization for Access by Provider's Staff Members following Termination.

1.5.2 End User Management

In administering or authorizing Access accounts for End Users, Provider will: (a) follow existing Client help desk procedures, or procedures subsequently agreed to by Client, for provisioning, maintaining or terminating Access accounts; (b) configure new passwords to be pre-expired and instruct End Users to use or change them immediately; and (c) establish additional controls, if not already in place, for validating End Users' identities against information repositories (e.g., Client global directory entries) so that passwords or other means of Access are delivered only to authorized End Users. If circumstances require workstation validation without an End User present, Provider will reset such End User's password to a pre-expired value.

1.5.3 Client Access Control

Client will retain, and may exercise in its sole discretion, the capability to independently grant, override, suspend, or terminate Access by any Provider's

Staff Members, Subcontractor, Client's Staff Members, or any other End User at any time; provided, however, that to the extent that Client's exercise of such capability materially adversely affects Provider's ability to perform the Obligations or provide the Services, including meeting Service Level Agreements, Provider will be excused. However, Provider will not be excused from its performance of any Obligation or provision of any Services, including any Service Level Agreements, pursuant to this Section 1.5.3 unless Provider has first notified Client that Client's exercise of its rights under this Section has materially adversely affected, or is expected to materially adversely affect, Provider's ability to perform the Obligation or provide the Service.

1.5.4 Client Verification Policy

Verification of End Users' identities by Provider will be conducted in accordance with the Client's Policies. Provider will put in place processes to: (a) specify, authorize, implement, monitor, and report on Access requests in accordance with the Client's Policies; and (b) investigate and report to Client all Access attempts that are rejected or fail for any reason.

With respect to Client e-mail accounts assigned to Provider's Staff Members: (a) Provider's Staff Members will not be granted Client e-mail accounts unless necessary to fulfill their roles and responsibilities; (b) e-mail from such accounts may not be sent or received by Provider's Staff Members over the Internet without the express written permission of Client; (c) e-mail capabilities from the Internet to these accounts (or any changes in such capabilities) must be justified on a case-by-case basis and have Client's prior written authorization (which will not be unreasonably withheld or delayed); (d) directory entries will indicate the status and employer of each individual; and (e) no e-mail systems are permitted to be used within the Client environment other than [Microsoft Outlook, or Lotus Notes, or Eudora, or AOL, etc.], unless authorized in writing by Client.

1.6 Record Retention

1.6.1 Back-Up

Provider shall employ procedures for creating back-up copies of all Work Product and storing related Records at a separate facility, under processes acceptable to Client. All back-up copies shall be considered Work Product under this Agreement. Provider shall also cause the periodic testing of all Records maintained in any back-up facilities to assure their continued integrity and quality for the performance of the Obligations and provision of the Services, including the use of appropriate Security Controls. Provider shall cause all Records related to the performance of the Obligations and the provision of the Services, including all Work Product, on a regular basis and in a form accessible and usable in the event of a suitable need, to be duplicated and stored at a facility that is not physically located in an area near Provider's premises.

1.6.2 Provider Record Keeping Requirements

Provider shall create, store, maintain and preserve all Records in connection with Provider's performance under this Agreement that are required: (a) by this Agreement, (b) to comply with the Controlling Rules or (c) to verify Provider's compliance with this Agreement (collectively, the "Provider Records"). Provider shall maintain all its Records relating to this Agreement, the Obligations and the Services in accordance with any applicable Client's Policies specifically identified by Client for such purposes.

1.6.3 Provider Record Audit Rights

During the Term and for a period of four years after Termination, upon written notice by Client to Provider, Provider shall promptly make available to Client and its auditors all Provider Records. Audits by Client shall not interfere unreasonably with Provider's business activities and shall be conducted at Provider's facilities during normal business hours. Provider acknowledges that this Agreement and all Records maintained by Provider shall be available to Client and any Person authorized by Client to conduct any audit or comparable examinations contemplated by this Section or other provisions of this Agreement. In the event any Person other than Client requests or demands to inspect any Provider Records, Provider shall: (a) immediately notify Client of such request or demand; and (b) comply with Client's instructions regarding (i) whether to permit or refuse the inspection and (ii) if Client authorizes the inspection, the procedures that will govern the conduct of the inspection. Notwithstanding the immediately preceding sentence, Provider reserves the right to permit inspection of the Provider Records by any Person in the event that Provider is advised by its legal counsel that Provider will likely be liable for its refusal to permit such inspection to such Person, provided that Provider (y) delivers on a timely basis to Client notice of the request or demand for inspection and a copy of any such opinion of Provider's legal counsel and (z) limits the scope of any such inspection to only that deemed necessary by its legal counsel to avoid the potential liability to such Person.

1.6.4 Copy of Provider Records, Data, Documentation and Work Product

Promptly after receipt of a request from Client, and in no event more than three business days after such request, Provider shall provide Client a copy of all Provider Records, Data, Documentation and Work Product in Provider's possession. In complying with its Obligations under this Section, Provider shall comply with all reasonable requests of Client with respect to format and delivery of the foregoing.

2. "Non-Core" Information Security-Related Provisions

2.1 Insurance; Allocation of Risk

2.1.1 Insurance Requirements

Provider shall maintain insurance of the kinds and in the amounts specified below with insurers of recognized responsibility, licensed to do business in the jurisdictions where the Obligations are to be performed, and having a Standard & Poor's rating of __ or its equivalent. Provider shall maintain the following insurance coverages:

> Cyber Insurance: Coverage for losses resulting from network security or loss incidents of the Provider or involving any Obligations, Deliverables, Services, Work Product, Client Information or other Resources in electronic form, or causing network disruptions in the performance of any of the Obligations, including but not limited to losses arising from transmission of Malicious Code, Denial of Service attacks or the unauthorized use or access to the Provider's systems or to Client's systems if arising out of the Obligations. The policy shall have a limit of liability of not less than $___ per occurrence and $___ in the aggregate.
>
> Comprehensive or Commerical General Liability Insurance: Coverage for losses result from property damage, bodily injury and personal

injury to others. The policy shall have a limit of liability of not less than $___ per occurrence and $____in the aggregate.

[Insert description of other applicable coverages.]

A combination of primary and excess/umbrella liability policies will be acceptable to meet the limits of the Comprehensive or Commercial General Liability Insurance above.

THE REQUIRED MINIMUM LIMITS OF INSURANCE COVERAGE SET FORTH ABOVE SHALL NOT IN ANY WAY RESTRICT OR DIMINISH PROVIDER’S LIABILITY UNDER THIS AGREEMENT. Provider shall also maintain a fidelity bond protecting Client from losses sustained as a result of fraudulent or dishonest acts committed by Provider’s employees acting alone or in collusion with other Persons. Provider’s insurance policies are to be primary and shall contain cross-liability and severability of interest provisions.

2.1.2 Client as “Additional Insured”

Certificates of such insurance shall be submitted to Client naming Client as an “additional insured” on such policies as appropriate, before the commencement of performance of any Obligations. These certificates shall certify that no material alteration, modification or termination of such coverage shall be effective without at least 30 days advance notice to Client.

2.1.3 Further Assurances

Should Provider at any time neglect or refuse to provide the insurance required, or should such insurance be canceled or not renewed, Client shall have the right to purchase such insurance, and the cost shall be billed to Provider. In addition, should Provider at any time neglect or refuse to pay the necessary premium, Client shall have the right to deduct this amount from monies due Provider under this Agreement.

2.1.4 Subcontractors

In the event Subcontractors perform any of the Obligations or provide any of the Services, Provider shall ensure that any agreement under which such Subcontractors are engaged include provisions requiring each Subcontractor to obtain insurance coverage that complies with the requirements above, unless Client specifically waives or modifies any of such requirements in writing in connection with Client's approval of such Subcontractor.

2.1.5 Waiver of Rights of Recovery

Provider will ensure that all policies of insurance that are in any way related to the Obligations or the Services and that are secured and maintained by Provider (or any of its approved Subcontractors or agents) include clauses providing that every underwriter will waive all of its rights of recovery under subrogation or otherwise, against Client, Provider and their subcontractors, agents or Affiliates. Provider waives all rights of recovery against Client and Client's Subcontractors, agents or Affiliates that Provider may have or acquire because of deductible clauses or the inadequacy of limits of any policies of insurance that are secured and maintained by Provider. Provider shall require all of its approved Subcontractors to waive the rights of recovery (as the aforesaid waiver by Provider) against Client, Provider and their other subcontractors, agents or Affiliates and deliver evidence of such waiver to Client before such Subcontractors perform any Obligations or provide any Services.

2.1.6 No Limitation of Liability

Nothing in this Section 2 shall be construed as limiting Provider's (or any Subcontractor's) liability to Client or any third party. The mere purchase and existence of insurance does not reduce or release Provider from liability incurred or assumed under this Agreement. Failure by Provider or any Subcontractor to maintain insurance shall not relieve it of liability under this Agreement.

2.1.7 Claims

Provider shall promptly make a full written report to Client as to all insurance claims arising from or in connection with: (a) the performance of the Obligations or provision of the Services, or (b) the presence of Provider's Staff Members on Client's premises. Provider shall cooperate fully with Client and with any insurance carrier in the investigation and defense of all such accidents and claims, such Obligation to survive Termination.

2.1.8 Financial Assurances

Upon Client's request (to be made not more than once per year), Provider shall provide Client with, or instruct Client as to how to access, publicly available financial information of Provider that will allow Client to assess Provider's creditworthiness. Provider shall not be obligated to provide Client with any nonpublic financial information unless it is requested by an officer of Client in writing. In the event Client reasonably determines Provider's creditworthiness is inadequate after a review of the relevant financial information, Client may terminate (a) this Agreement or (b) any or all outstanding Orders.

2.2 Audits

2.2.1 General

Provider will maintain a complete audit trail of all financial and non-financial transactions resulting from this Agreement. Provider will provide Client and Client's Affiliates (including the internal audit staff and external auditors of Client and Client's Affiliates), as well as Client's Regulators and other representatives or designees of Client as Client may from time to time designate in writing, with access, at any time and without restriction (except as provided in this Agreement) to all of the following for the purpose of performing examinations, tests, reviews, evaluations, audits or inspections (collectively, "audits," and those who perform audits, "auditors") of either Provider or any of its Subcontractors or Affiliates: (a) each Facility or part of a Facility at or through which Provider or any Subcontractor is performing Obligations or providing Services; (b) Provider's Staff Members; (c) data and Records relating to the Services; and (d) other facilities, personnel, data or Records as requested by Client or Client's Regulators.

2.2.2 Scope

At the discretion of Client, its Affiliates or its Regulators, and without limitation, audits may include reviews and evaluations of Provider's and Subcontractors' (a) standards, practices and procedures; (b) Systems, Equipment and software; (c) supporting information and calculations regarding compliance with SLAs and other performance standards; (d) general controls and security practices and procedures; (e) disaster recovery and back-up procedures; (f) efficiency in performing the Obligations and providing the Services, to the extent any of the

Obligations are performed or Services are provided on a specified rates or other time and materials basis; and (g) other Information or Data as (i) required by Regulators or (ii) necessary to enable Client (A) to meet, or to confirm that Provider is meeting, applicable regulatory requirements and other requirements of Applicable Law; (B) to confirm that Provider is complying with the Client's Policies and Provider's Policies; and (C) to confirm or evaluate any other aspect of Provider's or any Subcontractor's performance of the Obligations or provision of the Services.

2.2.3 Frequency/Timing

Except as otherwise provided in this Agreement, Client and its Affiliates will have the right to conduct audits [annually, semi-annually, quarterly, etc.] during the Term and for the longer of two years following Termination or the period Provider is required hereunder or by Applicable Law or Policies to maintain records to (a) verify the accuracy of all charges, invoices and credits under this Agreement; (b) verify the integrity of Client Information and examine the Systems that process, store, support and transmit that Information; and (c) verify Provider's and its Affiliates' and Subcontractors' performance of the Obligations, provision of the Services and conformance to this Agreement. To the extent required by Applicable Law or by a Regulator, Client may also, at any time, perform spot checks or otherwise perform random, unannounced testing of any aspect of Provider's compliance with Client's security requirements as relates to Provider's performance of the Obligations or provision of the Services or to any Facilities, Systems, Equipment or Records (excluding background information) pertaining to Provider's Staff Members or Subcontractors, used by Provider in the performance of the Obligations or the provision of the Services.

2.2.4 Notice and Procedures

Unless otherwise required by a Regulator: (a) Provider will be provided a minimum of three business days' notice of audits to be performed pursuant to this Section 2.2; (b) audits will be conducted during regular business hours (except with respect to Obligations that are performed or Services that are provided during off-hours) and in such a fashion so as not to unreasonably interfere with Provider's ability to perform Obligations or provide Services for Client or for other customers of Provider; and (c) auditors must comply with all applicable reasonable Provider and Subcontractor security and confidentiality requirements including, where appropriate, execution of a non-disclosure agreement reasonably acceptable to Provider or the relevant Subcontractor. Subject to the foregoing, auditors will be provided access to shared Systems or shared Provider or Subcontractor Facilities used in the performance of the Obligations and provision of the Services, provided that this will not be construed to give auditors access to any data of any customer of Provider or any Subcontractor other than Client or a Customer. Auditors will not have access to Provider's cost data except for (y) data on costs and expenses that are the financial responsibility of Provider under this Agreement, and (z) timesheets and similar substantiating data on the validity of the calculation of the charges that are charged on a project rates basis. Provider will cooperate with Client and Client's Regulators in connection with each audit, and Provider will provide the Auditors such assistance as they require, including installing and operating audit software.

2.2.5 Provider Audits

Provider will conduct Audits, including information security Audits, of or pertaining to the Obligations and the Services in such manner and at such times as is consistent with the audit practices of well-managed operations performing obligations and providing services similar to the Obligations and the Services.

2.2.6 Auditor Compensation

No external auditors selected by Client to perform any audits in connection with this Agreement may be compensated on a contingency basis.

2.2.7 Audit Follow-up

Following each Client audit: (a) Client will conduct, or will request its external auditors or examiners to conduct, an exit conference with Provider to obtain factual concurrence with issues identified in such audit or examination; (b) Provider and Client will meet to review each audit report (whether such audit was conducted by Client or a Regulator) promptly after the issuance thereof; (c) with respect to any findings by the related audit of any failure by Provider to comply with the requirements of this Agreement (including any Provider's Policies, Client's Policies, or Applicable Law, or with respect to the performance of the Systems, the provision of the Services, the performance of the Obligations, or any operations or procedures used to perform the Obligations or provide the Services, or with respect to a failure by Provider or any Subcontractor to take commercially reasonable efforts with respect to Information security), Provider will immediately implement corrective or remedial action, at no additional cost to Client and without referring any dispute regarding the need to take corrective action to the dispute resolution procedures set forth in this Agreement. Without limiting the generality of the foregoing, if Client determines that any Systems, procedures, policies or standards used in performing the Obligations or providing the Services conflict with, interfere with, or do not support compliance with the Client's Policies, then Provider will modify the same as reasonably required by Client. Provider will demonstrate any corrections, remedies or modifications to Client's reasonable satisfaction. If there is any dispute as to whether a failure that may be corrected, remedied or otherwise resolved by modifications has occurred, Client may request Provider to implement such change as soon as practicable, and the Obligations will be performed and the Services will be provided with such change in effect, notwithstanding the existence of a disagreement that may be resolved as provided in the dispute resolution procedures set forth in this Agreement. With respect to any other findings within any such audit report that reveal that any Client Information in Provider's or any Subcontractor's custody or control is exposed to a present risk of loss, corruption, damage, theft or any other comparable information security risks, Client will have the right to require changes be implemented to the Services in this regard and the Parties cooperate to evaluate and, if appropriate, mutually agree upon the appropriate manner, if any, in which to address the costs or impacts on Obligations or Services resulting from implementing such changes. If Provider is later able to demonstrate that the audit findings were inaccurate, that the cause of any failure or undesirable audit findings were not the result of a failure by Provider or any Subcontractor, or that the subsequent steps Provider took in response to the audit findings were unwarranted, Provider will be compensated for its time and materials expended in implementing changes required by Client on a project rates basis.

In the case of an audit, test, inspection or examination undertaken or commissioned by Provider (including by internal audit staff or external auditors) and relating to Provider's operating practices and procedures, if any such audit, test, inspection or examination reveals an adverse impact on the Services or on Client, Provider will make available promptly to Client the relevant portions of such audit, test, inspection or examination directly relating to the Services or the Obligations.

2.2.8 Invoice Adjustments

If any audit reveals any error or incorrect charging in any Provider invoice, the following will apply: (a) if Provider has overcharged Client, Provider will promptly make an appropriate correcting payment to, or credit to, Client together with interest on such amounts at the rate of ___% applied from the date of Client's payment of such amounts to Provider until Provider pays such amounts back to Client or credits them to Client; (b) if Provider has undercharged Client, Client will promptly make an appropriate correcting payment to Provider, provided that (i) Client will not be responsible for paying interest on any such undercharged amounts; and (ii) such payments will not relate to a period more than one hundred and eighty (180) days prior to the date of the audit.

2.3 Regulatory Compliance of Obligations and Services

Provider will perform all the Obligations and provide all the Services in compliance with all applicable Controlling Rules, including all regulatory requirements applicable to Client. Provider will implement, as part of the Services, processes to: (a) implement changes in regulatory requirements as required by Client pursuant to this Agreement; (b) identify any failure by Provider to comply with Controlling Rules and promptly report any known failures to Client; (c) communicate to Client descriptive information regarding processes adopted by Provider to implement regulatory compliance, to the reasonable satisfaction of Client; (d) take corrective action, as instructed by Client, with respect to any breaches of regulatory compliance; and (e) cause Provider's Staff Members and Subcontractors to comply with the Controlling Rules as they relate to the performance of the Obligations and the provision of the Services.

Part IV

Annex of Selected Information Security Resources

This Annex presents a selection of resources that can be relied upon in connection with studying or using this Guide. There are many different possible resources to be included in this selection and, for those included, many possible arrangements. No particular endorsement is intended by the fact the listed materials have been included, nor is the exclusion of any specific materials meant to diminish their possible utility.

The Internet Security Alliance joins with many other organizations in valuing the importance of standards and best practices as strong resources to be employed for improving information security. In addition, considerable work has been done by governments, notably the United States National Institute for Standards and Technology, which provide useful guidance. These materials are intended to highlight the organizations, standards and publications often recognized as those on which many companies and industries rely.

This Annex was prepared in December 2005; users are reminded that additional useful resources may become available after that date and that publications referenced here may be subsequently updated or revised.

Organizations

The following organizations maintain Internet-accessible resources addressing information security management:

Internet Security Alliance	www.isalliance.org
Information Systems Security Association	www.issa.org
The Information Systems Audit and Control Association	www.isaca.org
Organization for Economic Cooperation and Development	www.oecd.org
International Chamber of Commerce	www.iccwbo.org
World Bank	www.worldbank.org

Carnegie Mellon University Software Engineering Institute	www.sei.cmu.edu
Japanese Computer Security Association	www.jcsa.or.jp

Standards

The following standards organizations have published standards addressing information security management:

International Organization for Standardization	www.iso.org
British Standards Institute	www.bsi.org.uk
American National Standards Institute	www.ansi.org
Bundesamt für Sicherheit in der Informationstechnik	www.bsi.bund.de

Publications

The following publications may be useful in providing greater in-depth discussion of the management issues relating to information security.

Management Guides

Internet Security Alliance Common Sense
Guide for Senior Managers (July 2002)
http://www.isalliance.org

Building Security in the Digital Resource:
An Executive Resource – Business Roundtable
(November 2002)
www.businessroundtable.org

Information Security for Executives –
Business and Industry Advisory Committee
to the OECD, and International
Chamber of Commerce (ICC) (November 2003)
http://www.iccwbo.org/home/e_business/word_documents/SECURITY-final.pdf

ICC Handbook on Information Security Policy for
Small to Medium Enterprises (April 2003)
www.iccwbo.org

IT Baseline Protection Manual - P BSI 7152 E 1, BSI -
Bundesamt für Sicherheit in der Informationstechnik
http://www.bsi.bund.de/gshb/english/menue.htm

Governance Guides

Information Security Governance:
Toward a Framework for Action (Business Software Alliance)
http://www.bsa.org/resources/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=5841

Information Security Oversight:
Essential Board Practices (Nat'l Assoc of Corporate Directors)
http://www.nacdonline.org/publications/pubDetails.asp?pubID=138&user=6158BBEB9D7C4EE0B9E4B98B601E3716

IT Governance Implementation Guide
http://www.isaca.org/Template.cfm?Section=Browse_By_Topic&Template=/Ecommerce/ProductDisplay.cfm&ProductID=503

Turnbull Report - Internal Control -
Guidance for Directors on the Combined Code – Institute of Chartered Accountants in England & Wales (ICAEW)
http://www.icaew.co.uk/index.cfm?AUB=TB2I_6242,MNXI_47896

Internet Security Alliance
2500 Wilson Boulevard
Arlington, VA 22201-3834
United States of America
(t) 703/907-7708 (f) 703/907-7093
www.isalliance.org