INTERNATIONAL STANDARD

ISO/IEC 27033-3

First edition
2010-12-15

Information technology — Security techniques — Network security —

Part 3:
Reference networking scenarios — Threats, design techniques and control issues

Technologies de l'information — Techniques de sécurité — Sécurité de réseau —

Partie 3: Scénarios de réseautage de référence — Menaces, techniques conceptuelles et questions de contrôle

Reference number
ISO/IEC 27033-3:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 2

5 Structure 3

6 Overview 4

7 Internet access services for employees 6
7.1 Background 6
7.2 Security threats 7
7.3 Security design techniques and controls 7

8 Business to business services 9
8.1 Background 9
8.2 Security threats 9
8.3 Security design techniques and controls 10

9 Business to customer services 11
9.1 Background 11
9.2 Security threats 11
9.3 Security design techniques and controls 12

10 Enhanced collaboration services 13
10.1 Background 13
10.2 Security threats 14
10.3 Security design techniques and controls 14

11 Network segmentation 15
11.1 Background 15
11.2 Security threats 15
11.3 Security design techniques and controls 15

12 Networking support for home and small business offices 16
12.1 Background 16
12.2 Security threats 16
12.3 Security design techniques and controls 17

13 Mobile communication 18
13.1 Background 18
13.2 Security threats 18
13.3 Security design techniques and controls 19

14 Networking support for travelling users 20
14.1 Background 20
14.2 Security threats 20
14.3 Security design techniques and controls 20

15 Outsourced services 21
15.1 Background 21
15.2 Security threats 21
15.3 Security design techniques and controls 22

Annex A (informative) **An Example Internet Use Policy** 23

Annex B (informative) **Catalogue of Threats** 27

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference network scenarios — Threats, design techniques and control issues*

The following parts are under preparation:

— *Part 4: Securing communications between networks using security gateways — Threats, design techniques and control issues*

— *Part 5: Securing virtual private networks — Threats, design techniques and control issues*

There may be future parts to cover topics such as local area networks, wide area networks, wireless and radio networks, broadband networks, voice networks, Internet Protocol (IP) convergence (data, voice, video) networks, web host architectures, Internet email architectures (including outgoing online access to the Internet, and incoming access from the Internet), and routed access to third party organizations.

Information technology — Security techniques — Network security —

Part 3:
Reference networking scenarios — Threats, design techniques and control issues

1 Scope

This part of ISO/IEC 27033 describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. Where relevant, it includes references to ISO/IEC 27033-4 to ISO/IEC 27033-6 to avoid duplicating the content of those documents.

The information in this part of ISO/IEC 27033 is for use when reviewing technical security architecture/design options and when selecting and documenting the preferred technical security architecture/design and related security controls, in accordance with ISO/IEC 27033-2. The particular information selected (together with information selected from ISO/IEC 27033-4 to ISO/IEC 27033-6) will depend on the characteristics of the network environment under review, i.e. the particular network scenario(s) and ‘technology’ topic(s) concerned.

Overall, this part of ISO/IEC 27033 will aid considerably the comprehensive definition and implementation of security for any organization's network environment.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27033-1 and the following apply.

3.1
malware
malicious software
category of software that is designed with a malicious intent, containing features or capabilities that could potentially cause harm directly or indirectly to the user and/or the user's computer system

NOTE See ISO/IEC 27032.

3.2
opacity
protection of information that might be derived by observing network activities, such as deriving addresses of end-points in a voice-over-Internet-Protocol call

NOTE Opacity recognizes the need to protect actions in addition to information.

3.3
outsourcing
acquisition of services by an acquirer to perform activities required to support the acquirer's business functions

3.4
social engineering
act of manipulating people into performing actions or divulging confidential information

4 Abbreviated terms

AAA	Authentication, Authorization and Accounting
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DNSSEC	DNS SECurity extensions
DoS	Denial of Service
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPsec	IP Security Protocol
OAM&P	Operations, Administration, Maintenance & Provisioning
OSI	Open Systems Interconnection
PDA	Personal Data Assistant
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer (Encryption and authentication protocol)
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

5 Structure

The structure of this part of ISO/IEC 27033 comprises:

- an overview of the approach to addressing security for each reference scenario listed in this part of ISO/IEC 27033 (clause 6);
- a clause for each reference scenario (clause 7-15), which describes
  - threats for the reference scenario,
  - a presentation of the security controls and techniques based on the approach in clause 6.

The scenarios in the document are ordered per the following framework where the objective is to evaluate a given scenario as a function of the:

- **type of user access**, whether the user is inside an enterprise, or the user is an employee who is accessing enterprise resources from outside, or the user is a consumer, vendor or business partner, and,
- **type of information resources accessed**, open, restricted or outsourced resources.

Thus, the framework helps present a consistent structure, and makes addition of new scenarios manageable, as well as justifies the need for the various scenarios presented in this part of ISO/IEC 27033.

Table 1 — Framework for Ordering Network Scenarios

		Users		
		Inside	**Employees from outside**	**Outside**
Accessed information resources	**Open**	- Internet access services for employees - Business to business services		- Business to customer services
	Restricted	- Enhanced collaboration services - Business to business services - Network segmentation - Networking support for home and small business offices	- Mobile communication - Networking support for travelling users	- Enhanced collaboration services - Business to business services - Business to customer services
	Outsourced	- Outsourced services		- Outsourced services

Thus, the order in which the scenarios are listed in this part of ISO/IEC 27033 is as follows:

- Internet access services for employees (clause 7);
- Business to business services (clause 8);
- Business to customer services (clause 9);
- Enhanced collaboration services (clause 10);
- Network segmentation (clause 11);
- Networking support for home and small business offices (clause 12);
- Mobile communication (clause 13);
- Networking support for travelling users (clause 14);
- Outsourced services (clause 15).

6 Overview

The guidance presented in this part of ISO/IEC 27033 for each of the identified reference network scenarios is based on the following approach.

- Review the background information and scope of the scenario.
- Describe the threats relevant to the scenario.
- Perform risk analysis on discovered vulnerabilities.
- Analyse the business impact of addressing the vulnerabilities.
- Determine the implementation recommendations for securing the network.

In order to address the security of any network, an approach that is systematic and provides an end-to-end evaluation is desirable. The complexity of such an analysis is a function of the nature and size of the network in scope. However, a consistent methodology is important to managing security, especially due to the evolving nature of technology.

The first consideration in a security assessment is the determination of assets that require protection. These can be largely categorized into infrastructure, services or application assets. However, an enterprise can chose to define their own categories, but the distinction is important because the exposure to threats and attacks is unique to each asset category or type. For instance, if a router is categorized an infrastructure asset, and Voice over IP as an end-user service, then a Denial of Service (DoS) attack requires a different consideration in each case . Specifically, the router requires protection against a flood of bogus packets on the router's physical port that can prevent or impede the transmission of legitimate traffic. Similarly, the VoIP service requires protection of the subscriber’s account/service information from deletion or corruption such that a legitimate user is not prevented from accessing the service.

Network security also entails protection of the various activities supported on the network, such as management activities; control/signaling messages; and end-user data (resident and in-transit). For example, a management GUI can be subject to disclosure as a result of unauthorized access (easy to guess administrator ID and password). The management traffic itself is subject to corruption due to forged OA&M commands with spoofed IP addresses of the operations systems, or disclosure by sniffing, or interruption due to a packet flood attack.

The approach of identifying assets and activities enables a modular and systematic consideration of threats. Each reference network scenario is examined against a known set of threats to ascertain which threats are applicable. Annex B provides a list of known industry threats. Although the list should not be viewed as exhaustive, it provides a starting point for any analysis. Once the threat profile for the network is derived, the vulnerabilities are analyzed to determine how the threats may be realized in the context of the specific asset under consideration. Such an analysis will help determine what mitigations are missing and what countermeasures need to be deployed to achieve the protection objectives. A countermeasure will reduce the likelihood of the threat being successful and/or reduces its impact. Risk analysis that analyzes the risk represented by discovered vulnerabilities. Business impact analysis consists of arriving at a business decision regarding how to address each vulnerability: remediate, accept risk, or transfer risk.

Designing countermeasures and implementing controls for protecting vulnerabilities against threats is part of any security assessment methodology. In accordance with the ISO/IEC 27000 series standard, the selection and implementation of relevant controls is critical to asset/information protection. The standard requires the preservation of confidentiality, integrity and availability of information, and specifically states that in addition, other properties such as authenticity, non-repudiation and reliability can also be involved.

The following is a set of security properties that is used in this part of ISO/IEC 27033 to develop mitigations and countermeasures in an objective manner. The rationalization for the need for each security property (in addition to confidentiality, integrity and availability) is described below.

- Confidentiality is concerned with protecting data from unauthorized disclosure.
- Integrity is concerned with maintaining the correctness or accuracy of data and protecting against unauthorized modification, deletion, creation, and replication.
- Availability is concerned with ensuring that there is no denial of authorized access to network elements, stored information, information flows, services, and applications.
- Access Control provides, through the use of authentication and authorization, control to enforce access to network devices and services, and ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. For example, in an IPTV deployment, one of the known security recommendations, disabling the debugging interface on subscriber set top boxes, is derived from a consideration of the access control property. A review of confidentiality, integrity or availability will not result in some other recommendations.
- Authentication is concerned with confirming or substantiating the claimed identity of a user or communicating parties when used by access control for authorization, and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. For instance, an individual may gain access to a network management system, but will need to be authenticated in order to update subscriber service records. Thus the ability to perform network management activities cannot be assured by simply addressing confidentiality, integrity, availability, or access control.

NOTE In Role-Based Access Control, authorization takes place by virtue of the user being assigned to a role. Access control then verifies the user has the role prior to granting access. Similarly, access control lists grant access to anything that satisfies the policy, so if you satisfy the policy requirements you are authorized access. The authentication and authorization functions are null in this case.

- Communication or Transport Security is concerned with ensuring that information only flows between authorized end-points without being diverted or intercepted.
- Non-repudiation in concerned with maintaining an audit trail, so that the origin of data or the cause of an event or action cannot be denied. Identifying the authorized person that performed an unauthorized action on protected data has nothing to do with the data's confidentiality, integrity, availability.
- Opacity is concerned with protecting information that might be derived from the observation of network activities. Opacity recognizes the need to protect actions in addition to information. Protecting information is addressed by confidentiality. Protecting the conversation in a phone call between Person A and Person B protects their confidentiality. Protecting the fact that Person A and Person B had a phone call ensures opacity.

In all the scenarios described in this part of ISO/IEC 27033, the above-stated security properties are reviewed as part of the security design technique and control phase. Table 2 below shows examples of network security mechanisms that can be implemented for security properties that are selected for mitigating the potential risk.

Table 2 — Example Network Security Techniques

Security Considerations	**Security Mechanisms / Techniques**
Access Control	Physical badge system, Access Control Lists (ACL), Separation of duties
Authentication	Simple log-in/password, Digital certificates, Digital Signatures, TLSv1.2, SSO, CHAP
Availability	Redundancy & back-up, Firewalls, IDS/IPS (for blocking DoS), Business continuity, Managed network & services with SLAs
Communication Security	IPsec / L2TP, Private Lines, Separate networks
Confidentiality	Encryption (3DES, AES), Access control lists, File permissions
Integrity	IPsec HMACs (e.g. SHA-256), Cyclic redundancy checks, Anti-Virus Software
Non-repudiation	Logs, Role based access control, Digital signatures
Opacity	Encryption of IP headers(for example: VPN with IPSec tunnel mode), NAT (for IPv4)

In this part of ISO/IEC 27033, the above considerations are inherent in the design and implementation discussed in the context of each reference network scenarios. Typically, an organization will select the relevant ISO/IEC 27002 controls to meet their business objectives, and the guidelines in this part of ISO/IEC 27033 are intended to provide the network level considerations required for the implementation of the chosen controls.

7 Internet access services for employees

7.1 Background

Organizations that need to provide Internet access services for their employees should consider this scenario so as to ensure access for clearly identified and authorized purposes, not general open access. Organizations need to be concerned about managing that access to avoid loss of network bandwidth and responsiveness as well as exposure to legal liability when employees have uncontrolled access to Internet services.

Controlling employee access to the Internet is a growing concern given the number of emerging Internet case laws. Thus an organization is responsible for establishing, monitoring and enforcing an unambiguous Internet Use Policy by evaluating the following scenarios, and providing relevant claims in the policy:

- Internet access is allowed for business reasons;
- if Internet access is also allowed in (limited) form for private purposes, which services are allowed to be used;
- if enhanced collaboration services are allowed;
- if employees are allowed to participate in chat channels, forums etc.

Even though often a written policy acts as a significant deterrent to unacceptable Internet usage, the organization is still subject to substantial information security risks. In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

7.2 Security threats

Security threats related to Internet access services for employees are:

- Virus attacks and introduction of malware:
  - o employees using the Internet are also a prime target for malware which may lead to, loss or corruption of information and loss of control of IT infrastructure, and a huge risk to an organization's network security;
  - o user downloaded files or programs may contain malicious code. Given the ubiquity of applications such as instant messaging, peer-to-peer file sharing, and IP telephony, employees can inadvertently download and install a malicious application that can evade network defences using such techniques as port agility (jumping around among open ports) and encryption. In addition, peer-to-peer applications can be exploited to serve as covert channels for botnets;
  - o vulnerabilities in web browsers or other web applications may be exploited by malware, and result in virus infections and installation of trojans. Once infected, availability can be severely impacted due to virus propagation activities leading to network overload. Trojans can enable unauthorized external access leading to confidentiality violations.
- Information leakage:
  - o applications that allow upload of information to web-based servers, may lead to uncontrolled transfer of data from inside an organization to the Internet. If encrypted sessions are used (e.g. TLS) then even logging of such activity may not be possible. Similar security risks are introduced when unauthenticated portable code is executed on systems inside an organization.
- Unauthorized usage and access:
  - o loss of control of infrastructure, systems and applications can result in fraud, denial of service, and abuse of facilities.
- Liability due to regulatory non-compliance:
  - o legal liability due to non-compliance with legislation or regulatory obligations;
  - o non-conformance with an organization's use policy can lead to regulatory non-compliance.
- Reducing network availability due to inadequate bandwidth or stability problems:
  - o excessive use of high bandwidth services such as streaming media or peer to peer file sharing may lead to network overload.

7.3 Security design techniques and controls

Security design techniques and controls related to employee internet access services are discussed in Table 3.

For a given security risk, each security property is reviewed for applicability in reducing the risk, and then a corresponding technical implementation example is presented in the second column. For example, integrity, access control, and authentication are applicable for protecting against malicious code.

Table 3 — Security Controls for Employee Internet Access Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Virus attacks and Introduction of Malware	
• Integrity • Access Control • Authentication	• Only provide the business relevant internet services towards the employee. Use of blacklists for authorized services, so as to not allow chat channels or web mail services, or peer-to-peer networking protocols. • Use of antivirus software on the gateways to the Internet for scanning all traffic from and to the Internet. Scanning should include all network protocols authorized for use. Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available. • Use of antivirus software on all client systems, especially those used for internet access by employees. • Scan files and all stored information for viruses and Trojans and other forms of malware. • Data/file integrity verification using algorithms such as hash/checksums, certificates. • Blocking pop-ups and web advertisements. • Routing of traffic used for Internet access services through a small number of controlled security gateways. • Active content authentication.
Information Leakage	
• Communication security • Integrity • Access Control	• Implementing Filters for mobile code on the gateways to the Internet. • Accept mobile code only from uncritical, white listed sites. • Accept only digital signed mobile code signed from approved Certification Authorities or from approved vendors, enable the respective configuration options on the client side, e.g. by actively manage and implement a white list of allowed code signing Certification Authorities.
Unauthorized Access and Usage	
• Access Control • Non-Repudiation	• Only provide the business relevant internet services towards the employee. Use of blacklists for unauthorized services, e.g. chat channels or web mail services. Implementation of filters for non authorized protocols, e.g. peer-to-peer networking protocols. • Restrict the use of services which easily enable the transfer of big amounts of data. • Ensure that proper logging and monitoring is in place for all services which allow the possibility to transfer data towards the Internet. • Clearly define authorized and unauthorized usage of internet access in a dedicated policy (see sample template in Annex A). • Ensure user awareness through adequate education and training. • Only provide the business relevant internet services towards the employee. Use of blacklists for unauthorized services, e.g. chat channels or web mail services. Implementation of filters for non authorized protocols, e.g. peer-to-peer networking protocols.
Liability due to Regulatory Non-Compliance	
• Non-Repudiation	• Usage logs, time stamps. • User awareness and training.

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Reducing Network Availability	
• Integrity • Availability	• Proper vulnerability management and patching of known system vulnerabilities within timeframes based on vulnerability criticality. • Focus of vulnerability management should be all systems receiving internet traffic, either on transport or application level, which includes all systems used in the context of the gateways used towards the Internet as well as end user systems used for accessing internet services, especially if they use a windows operating system. • Throttle bandwidth for streaming media (only if permitted per business policy). • Network and system resources should be monitored (IDS, logs, audits, etc.) to detect system, security, and operational events.

8 Business to business services

8.1 Background

Organizations that conduct transactions with other organizations, such as manufacturer, wholesaler, retailer, should consider this scenario

Traditionally business to business services have been implemented by using dedicated leased lines or network segments. The Internet and the related technologies do provide more options, but also introduce new security risks associated with the implementation of such services. The evolved business-to-business e-commerce model allows organizations to conduct business over the Internet, and the applications focus on using the Internet, extranet, or both to improve business partnerships in which the entities are known to each other and all users are registered, unlike the business to consumer scenario.

Typically business to business services have their own requirements. For example, availability and reliability are very important requirements as frequently organizations are directly dependent on working business to business services.

When using the Internet as a base network connection to implement business to business services, requirements such as availability and reliability need to be handled differently than before. Proven measures such as quality of service assumptions used, e.g. in conjunction with leased lines, do not work any more. The new security risks need to be mitigated by appropriate design techniques and controls. The focus is on reinforcing trust between organizations by preventing access to unauthorized data and maintaining separation of business systems.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage.

8.2 Security threats

Security threats related to business-to-business services are:

- Virus attacks and introduction of malware:
  - o malware exploits leading to infiltration of systems leading to disruptions or unauthorized access to sensitive information;
  - o vulnerabilities in web browsers or other web applications may be exploited by malware, and result in virus infections and installation of trojans.

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on business to business portals or extranets.
- Insider attacks by authorized business partners.
- Forgery of transaction contents (messages not reaching the intended recipient or data is tampered during transmission).

8.3 Security design techniques and controls

Information security design techniques and controls related to business-to-business services are associated with:

Table 4 — Security Controls for Business to Business Services Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Virus Attacks and Introduction of Malware	
• Integrity • Access Control • Authentication	• Use of virus checking software on the gateways to the Internet for scanning all traffic from and to the Internet. Scanning should include all network protocols authorized for use. Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available. • Scan files and all stored information for viruses and Trojans and other forms of malware. • Data/file integrity verification using algorithms such as hash/checksums, certificates. • Routing of traffic used for Internet access services through a small number of controlled security gateways. • Active content authentication.
Denial of Service Attacks	
• Availability • Opacity	• Disable unused protocol ports and services to prevent them from responding to unauthorized scans/probes, which has the potential of causing a traffic flood DoS. • Excluding descriptive information from warning banners prevents providing targeting information to attackers.
Insider Attacks	
• Access Control • Non-Repudiation	• Well defined security policy for access management (for business relationship management). • Clearly identified roles and responsibilities. • Customised warning banners. • Limit on privileges. • Logging of all critical/non-critical transactions by users.
Forgery of Transaction Contents	
• Non-Repudiation	• Detailed logs of transactions. • Use of digital signatures.

9 Business to customer services

9.1 Background

Organizations that conduct transactions with consumers should consider this scenario.

Business to customer services, also referred to as e-business services includes services such as e-commerce, e-banking, and e-government. In business to customer services, security must balance enabling transactions with preserving brand and business value.

The information security requirements include those associated with:

- confidentiality (especially regarding e-banking),
- authentication,
- integrity,
- data communications security where the end user expects the business service provide to protect the transaction path between the user and the provider. Resistance against sophisticated attacks (e.g. 'man in the middle' or 'man in the browser' attacks),
- Availability is an important dimension for the e-business provider.

The information security characteristics include:

- security only 'guaranteed' on the end platform typically under the control of an organization, providing a good environment for implementing controls and maintaining a good platform level security,
- security on the customer platform, often a PC, can typically be poor. It is harder to get controls implemented in such an environment, and thus customer platforms would present significant risks in this scenario (without a 'conditions for secure connection' set of requirements in a contract, which may be difficult to impose in such an environment).

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage.

9.2 Security threats

Security threats related to business to customer services are:

- Virus attacks and introduction of malware:
  - o malware exploits leading to infiltration of systems leading to disruptions or unauthorized access to sensitive information;
  - o vulnerabilities in web browsers or other web applications may be exploited by malware, and result in virus infections and installation of trojans.
- Unauthorized access:
  - o unauthorized access of back-end databases (e.g. SQL injection attacks, cross-site scripting attacks);
  - o account harvesting which is the ability to derive valid account information depending on how a web application responds to user's authentication attempts. Automated scripts are often used to harvest valid user ids and account names.
  - o online identity theft using successful social engineering attacks (through the use of deceptive techniques), such as phishing attacks and DNS-based attacks that connect users to fraudulent web-servers that look legitimate but are not;
  - o unauthorized access to systems or networks with malicious intent to copy, modify or destroy data;
  - o illegal content decryption leading to copyright violations and theft of content.

- Denial of service attacks.
- Forgery of transaction contents (messages not reaching the intended recipient or data is tampered during transmission).

9.3 Security design techniques and controls

Security design techniques and controls related to business to customer services are discussed in Table 5.

Table 5 — Security Controls for Business to Customer Services Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Virus Attacks and Introduction of Malware	
• Integrity • Access Control • Authentication	• Use of virus checking software on the gateways to the Internet for scanning all traffic from and to the Internet. Scanning should include all network protocols authorized for use. • Scan files and all stored information for viruses and Trojans and other forms of malware. • Data/file integrity verification using algorithms such as hash/checksums, certificates. • Routing of traffic used for Internet access services through a small number of controlled security gateways. • Active content authentication.
Unauthorized Access	
• Access Control • Authentication • Confidentiality • Communication Security • Integrity • Opacity	• Limit permissions of web applications when accessing backend databases. • Network segmentation and security tiers within a Demilitarized Zone (DMZ) to prevent direction connection paths to corporate data assets. • Secure user registration to ensure that access credentials are only issued to authentic users – such as using an independent Registration Authority for the process. • Authentication using digital certificates, passwords, biometrics or smartcards. • Firewalls and access control lists to prevent unauthorized user access. • Role based access control to limit the function the user is permitted to perform. • Web application log reviews for attack identification and containment. • Suitable levels of encryption of stored information. • Ensuring security between web browsers and web servers using technologies such as SSLv3/TLS. • Securing basic Web Service communication using for example SOAP messages. • Data/file integrity verification using algorithms such as hash/checksums, certificates. • For web application level data integrity of URLs, cookies or hidden form elements: o encrypt all data (even if SSLv3 is being used); o use timestamps with the variables; o digitally sign or use keyed hash for sensitive data. • Use of reverse proxy between the web server and the external network.

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Denial of Service Attacks	
• Availability • Opacity	• Disable unused protocol ports and services to prevent them from responding to unauthorized scans/probes, which has the potential of causing a traffic flood DoS. • Excluding descriptive information from warning banners prevents providing targeting information to attackers.
Forgery of Transaction Contents	
• Non-Repudiation	• Detailed logs of transactions. • Use of digital signatures.

10 Enhanced collaboration services

10.1 Background

Organizations that utilize services involving multiple employees should consider this scenario. Examples of such services are:

- Groupware
- File servers
- Mailing List
- Web-based services

Enhanced collaboration services, which integrate various communication and document sharing possibilities, are an important aspect for business environments.

Such collaboration services typically integrate video telephony, voice communication with chat channels, e-mail systems, as well as document sharing and online co-working environments.

There are two basic ways how to use such services for an organization:

- use them as internal services only, but with the disadvantage that the services cannot be used with external partners, etc.;
- use them as internal services and services external to an organization. This offers much more benefit from using such services, but at the same time has more associated security risks compared with only internal usage.

Regarding implementation, the services may be:

- implemented in-house, or
- from a third party.

If the services are to be used internally and externally, then buying in collaboration services from a third party may be a more appropriate solution.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage. The security controls apply to management, signalling and user traffic.

10.2 Security threats

Security threats related to enhanced collaboration services are:

- Unauthorized access leading to disclosure of sensitive information:
  - misuse of collaboration tools to illegally share copyrighted material, obtain confidential data, and expose users to undesirable content or propaganda;
  - violation of Opacity by monitoring usage patterns, spamming and identity attacks.
- Virus attacks and introduction of malware:
  - distribution and execution of malware by exploiting shared resources.
- Reducing Network Availability:
  - overloading the network with legitimate traffic;
  - exploiting protocol vulnerabilities used in the collaboration services.

10.3 Security design techniques and controls

Information security design techniques and controls related to enhanced collaboration services are associated with:

Table 6 — Security Controls for Enhanced Collaboration Services

Applicable Security Properties for Identified Threats	**Implementation Design and Technologies**
Unauthorized access leading to disclosure of sensitive information	
• Access Control • Authentication • Confidentiality • Communication Security • Non-Repudiation	• Role-based access to applications, networks, and storage • Assigning users in different roles to different VLANs with different permissions • Role based policies for usage rights and access to resources, such as applications that a user can run, • Access control lists • Strong authentication and authorization • VLANs for network virtualization • Host-based IDSs • Encryption of data
Virus attacks and introduction of malware	
• Integrity	• Use of screen transferring software such as Terminal Servers to minimize the data and potential malware to enter the corporate environment
Reducing Network Availability	
• Availability	• using virtual storage area networks to improve availability and security of data at rest, • prevention of information removal by using software tools to prevent copy/paste of information, block attempts to write to removable media, or printing, • monitoring software to detect policy violations – such as access violations of applications and other network resources

11 Network segmentation

11.1 Background

Organizations that wish to divide their internal network into multiple domains in to align with the organizational structure should consider this scenario.

Segmenting networks is a technique that can be used to augment system and application access controls. Network segmentation can be used to group certain types of activity, application, or systems in a way that access is only possible to those with access to the network segment. In this way, network access controls augment other end-point access controls and provides an additional level of defence in depth. For example, network segmentation can be used to:

- segregate administrative and maintenance capabilities from routine user access to business applications;
- segregate critical applications from other applications;
- segregate databases from most users.

For multi-national organizations country specific legislation has a great influence on information security requirements. To cover the different information security requirements for the countries an international organization is doing business in, segmentation of a network in effect in line with country borders can be an effective approach. For example, a particular country's legislation may require specific protection of customer/client data, and does not allow the transfer of such data to another country. This typically requires additional information security controls to guarantee compliance with such legislation.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage.

11.2 Security threats

Security threats related to network segmentation for fulfilling country-specific compliance requirements in international organizations are:

- Liability due to Regulatory Non-compliance;
- Data Leakage:
  - breach of confidentiality, e.g. when customer/client data is accessible from countries from which it should not,
  - breach of country specific privacy requirements,
  - reputation related risks implicated by not meeting customer/client expectations regarding confidentiality or opacity.

11.3 Security design techniques and controls

Information security design techniques and controls related to network segmentation for fulfilling country-specific compliance requirements in international organizations are associated with:

Table 7 — Security Controls for Network Segmentation

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Liability due to Regulatory Non-compliance	
• Opacity • Confidentiality	• Policy and User Awareness: o Privacy laws o Allowable encryption technologies o Data storage, transfer laws o Laws for lawful intercept
Data Leakage	
• Access Control • Authentication • Integrity	• Security Gateways • Application Level Proxies • Data Encryption

12 Networking support for home and small business offices

12.1 Background

Organizations that need to provide access to internal resources to their employees at home or small offices should consider this scenario.

Home and small business offices often require the extension of the internal network of an organization to a home or small business location. The costs of extensions to home or small business locations is a critical issue, since cost/benefit reflections typically do not require high implementation costs. This means cost limitations on the security controls to be used to secure such network extensions and typically prevents the use of established inter-networking security controls used to connect bigger Intranet segments.

In many home or small business scenarios the infrastructure may also be used for private as well as for business purposes – which may result in additional information security risks.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage.

12.2 Security threats

Security threats related to networking support for home and small business offices are:

- Unauthorized access:
  - o weak configuration settings in network access equipment, e.g. of SOHO routers (Small Office and Home Office),
  - o use of split-tunneling,
  - o missing or weak physical security controls,
  - o longer window of opportunity due to “always-on” nature of network connectivity,
  - o use of guest accounts and default settings.
- Virus attacks and introduction of malware:
  - o equipment, including PCs used in the home or small office network and operated with inadequate security controls, e.g. missing or weak malware protection etc.,

  - problems introduced by mixing private and business environments, e.g. by the private usage of protocols with inherent high risks, such as peer to peer file sharing protocols,
  - patching failure,
  - once infected, availability can be severely impacted due to virus propagation activities leading to network overload.

- Unauthorized disclosure of sensitive information:
  - lack of encryption of data stored on systems and transmitted in the home or small business network,
  - misuse of access possibilities such as WLAN access in the home or small business network,
  - lack of awareness and security best practices training of end-users,
  - invalidation of assumptions regarding the protection of Intranets, since the network gateways in home or small office environments do not provide the same protection level as gateways used to interconnect office branches.

12.3 Security design techniques and controls

Information security design techniques and controls related to networking support for home and small business offices are associated with:

Table 8 — Security Controls for Networking for Home and Small Business Office Scenario

Applicable Security Properties for Identified Threats	**Implementation Design and Technologies**
Unauthorized Access	
• Access Control • Authentication • Communication security	• Disable network interfaces and services that are not used • Install host-firewall - drop or reject all incoming connections from outside • Design and technology protections for split tunnelling • Systems should not utilize blank, null, or default passwords. • Strong passwords should be enforced for all users. Anonymous/ guest access should not be permitted. • Technical compliance checks to ensure proper configuration and setup of all security sensitive equipment, e.g. router or WLAN access points • Secure Virtual Private Network technologies in network access components such as network access routers
Virus Attacks and Introduction of Malware	
• Integrity • Availability	• Maintain current software versions and patch levels • Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available • Use host based Intrusion Detection System (HIDS) at least to detect software/database integrity (as applicable) • Scan files and all stored information for viruses and Trojans and other forms of malware • Backup of configuration data, and files for incident response and recovery
Unauthorized Disclosure of Sensitive Information	
• Confidentiality • Opacity	• User awareness and training for security best practices • Encryption of stored and transmitted data

13 Mobile communication

13.1 Background

Organizations that permit the use of mobile devices for employees should consider this scenario.

This scenario focuses on the security concerns of enterprises using and deploying mobile devices and applications. Although the main driver for the fast development of new features of mobile devices, such as smart phones or personal data assistants (PDAs), comes from the consumer market, these are also used in business environments. Often such devices are personally owned and used in both for business purposes and privately. Sometimes the devices may be company provided and are used for personal use. Thus, devices directed at the business market need to have features introduced for the consumer market, as the vendors want to gain as much business as possible in a competitive market.

The mobile communication devices allow remote users to synchronize personal databases, and provide access to network services such as wireless e-mail, Web browsing, and Internet access. When a person uses the same device for private as well as business purposes, there is a tendency to circumvent or disregard use policies, thus introducing significant information security risks to the enterprise.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage.

13.2 Security threats

Security threats related to mobile communication devices are:

- Unauthorized access of information stored on mobile devices due to:
  - inadequate access control or protection of sensitive information,
  - lack of awareness and inadequate passwords,
  - weak configuration,
  - hijacking attacks by rogue devices,
  - missing end user awareness of information security protection requirements, e.g. with mixing of private and business information.
- Unauthorized disclosure of sensitive data and location information:
  - location-based services can disclose user position information to unauthorized third parties, thus leading to privacy concerns,
  - eavesdropping,
  - involvement of inadequately protected third parties in the communications flow,
  - usage of plaintext or inadequately protected transmission protocols,
  - improper disposal procedures.
- Unauthorized modification/deletion of stored information (including software) due to:
  - introduction of malware by installation of software from unauthorized sources,
  - exploitation of vulnerabilities in the underlying operating system.
- Spam leading to:
  - increased service charges,
  - enabling phishing attacks,
  - DoS attacks.
- Theft or accidental loss, both of which could lead to:
  - loss of sensitive data whenever data stored on the device is not mirrored or backed up somewhere else,

- o confidentiality issues when sensitive data stored on the device is not adequately protected,
- o secure data backup.

13.3 Security design techniques and controls

Information security design techniques and controls related to personal mobile communication devices are associated with:

Table 9 — Security Controls for Mobile Communication Scenario

Applicable Security Properties for Identified Threats	**Implementation Design and Technologies**
Unauthorized access of information stored on mobile devices	
• Access Control • Authentication • Non-Repudiation	• User awareness for physical control • Avoiding default configurations • Strong authentication • Enabling logging options • Inactivity timer lock • Firewall • Organization security policy for passwords and business usage (restricting personal use for enterprise-owned devices)
Unauthorized disclosure of sensitive data and location information	
• Confidentiality • Authentication • Communication Security • Opacity	• Encrypting stored and transmitted (wireless) data • Password protection • Avoidance of third party services which require clear text access to transmitted data or, if not feasible, requesting assurance that confidentiality of processed data is as required, • Ensure secure synchronization procedures, • Secure VPN for remote access connections, • Proper disposal procedures for erasing sensitive data • User consent for location use
Unauthorized modification/deletion of stored information (including software)	
• Confidentiality • Availability • Integrity	• Disable unused wireless interfaces, services and applications, • Up-to-date patching of OS, • Proper disposal procedures for erasing sensitive data, • Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available • Software downloads only from enterprise software distribution system (avoiding installation of unlicensed software) • Digital signatures to verify download sources
Spam	
• Access Control	• Content filtering • Increasing user awareness
Theft or accidental loss	
• Confidentiality • Availability	• Remote asset management (disable/lock device) • Periodic secure backup • Centralized management for asset tracking and policy compliance

14 Networking support for travelling users

14.1 Background

Organizations that permit travelling employee to access the enterprise resources should consider this scenario.

Solutions and offerings in this area often focus on the functionality side and are targeted primarily to the consumer market. From an information security viewpoint, the offered functionality levels introduce new risks, e.g. by affecting or invalidating assumptions regarding information security. For example, an assumption of maintaining a well controlled and (from the outside) protected Intranet may be questioned substantially if travelling user access to the Intranet is not implemented with appropriate controls.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage.

14.2 Security threats

Security threats related to networking support for travelling users are:

- Unauthorized access:
  - misuse of travelling user network support to gain unauthorized access to the Intranet of an organization,
  - compromise of security gateways used on the Intranet network border,
  - unauthorized access to data stored on travelling user devices.
- Reducing network availability:
  - availability problems introduced when user expectations regarding network support cannot be met, e.g. when this is dependent on the availability of Internet Service Providers.

14.3 Security design techniques and controls

Information security design techniques and controls related to networking support for travelling users are associated with:

Table 10 — Security Controls for Networking Support for Travelling Users

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Unauthorized Access	
• Access Control • Authentication • Communication Security • Confidentiality	• enhanced authentication techniques (certificate based authentication, two-factor or challenge response authentication) • dedicated services for travelling users based on TLS/SSLv3 protected Web interfaces • using Secure Virtual Private Network technologies combined with appropriate security gateways on the client systems (e.g. personal firewalls): o layer 2/3 implementations, e.g. IPsec, o application level VPN's, e.g. based on TLS • encryption of stored user data
Reducing Network Availability	
• Availability	• engaging service providers with a global and using service level agreements for reliability and performance

15 Outsourced services

15.1 Background

Organizations that use outsourced services should consider this scenario.

Organizations use outsourced services because it is viewed as a viable business strategy, but it also introduces organizational and operational complexities, specifically for ensuring the quality and security of outsourced services.

The extended enterprise inherits additional risk because of the dependency on the service provider. For instance, service providers or vendors can require direct access to assets inside an enterprise for support and/or incident management issues, thus exposing critical assets to security risks. Whilst many support services require permanent access rights to the supported infrastructure, others may only need temporary access. Often support services need highly privileged access rights in order to fulfil their tasks.

Regardless of the type of outsourcing scenario, security considerations and oversight is required in all such contractual arrangements. A general view of threat and concerns is presented is this document. More in-depth information about securing outsourced services can be found in ISO/IEC 27036.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate the associated risks are described for internal, and internal plus external, usage.

15.2 Security threats

Security threats related to outsourced services are:

- Unauthorized access to other internal systems (when supplier accesses internal systems for remote support and maintenance):
  - abuse of remote maintenance ports,
  - abuse of administrator rights.
- Unauthorized disclosure of sensitive data by service provider:
  - lack of respect for intellectual property rights,
  - lack of separation of multi-customer environments,
  - lack of information security best practices (for example, password sharing may be rampant),
  - mishandling of storage media,
  - use of non-secure communications methods.
- Introduction of malware (in software development environments):
  - inadequate security in software development and software release procedures,
  - insecure transfer of files and data,
  - insecure online collaboration practices.
- Liability due to regulatory non-compliance:
  - lack of understanding of country specific regulatory and liability laws if the service provider is based in a different country,
  - insufficient legal data privacy and protection requirements applicable in the country where the supplier is located; it may have a substantial adverse effect on the data privacy and protection requirements applicable to the acquirer.

15.3 Security design techniques and controls

Information security design techniques and controls related to external or outsourced services are associated with:

Table 11 — Security Controls for Outsourced Services

Applicable Security Properties for Identified Threats	**Implementation Design and Technologies** (implementation can be assumed by the outsourcing organization or outsourced enterprise depending on statement of work)
Unauthorized Access to internal systems	
• Access Control • Authentication • Non-Repudiation	• Strict assignment of individual user ids • Strong authentication (e.g., two-factor authentication) for root/admin login • On-site console port or craft port protected by userID and password (in case service provider requires on-site physical access) • Comprehensive logging of access activities, and log reviews
Unauthorized Disclosure of Sensitive Data	
• Confidentiality	• Client data protection best practices through encryption • Security awareness and training • Monitoring and audit facilities and procedures • Contractual security policy and procedures directives
Introduction of malware	
• Integrity	• Secure coding practices • Change management processes • Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available
Liability due to Regulatory Non-compliance	
• Confidentiality • Opacity	• Awareness of local regulations • Use of compliant encryption software • Opacity mechanisms (IPsec VPNs)

Annex A
(informative)

An Example Internet Use Policy

A.1 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>'s established culture of openness, trust and integrity. InfoSec is committed to protecting <Company Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every <Company Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

A.2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

A.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

A.4 Policy

A.4.1 General Use and Ownership

1. While <Company Name>'s network administration desires to provide a reasonable level of opacity, users should be aware that the data they create on the corporate systems remains the property of <Company Name>. Because of the need to protect <Company Name>'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Company Name>.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.
5. <Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

A.4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
6. Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the <Company Name> Internet/Intranet/Extranet, whether owned by the employee or <Company Name>, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. Employees should use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

A.4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

A.4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Company Name>.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Company Name> or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a <Company Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any <Company Name> account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

A.4.3.2 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

A.4.4 Blogging

1. Blogging by employees, whether using <Company Name>'s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of <Company Name>'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>'s policy, is not detrimental to <Company Name>'s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>'s systems is also subject to monitoring.
2. <Company Name>'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or

otherwise engaging in any conduct prohibited by <Company Name>'s Non-Discrimination and Anti-Harassment policy.

4. Employees may also not attribute personal statements, opinions or beliefs to <Company Name> when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of <Company Name>. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, <Company Name>'s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging activity

A.5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A.6 Definitions

Term	**Definition**
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

A.7 Revision History

Annex B
(informative)

Catalogue of Threats

B.1 Misrepresenting Authority & Rights:

- Presentation of a false authority as if it were true with the intent to mislead.
- Presentation of a password, key or certificate of another (e.g., system administrator).
- Unauthorized acquisition and use of subscriber service-related authentication information (e.g., user id/password, session keys). Limited to individual subscribers.
- Unauthorized acquisition and use of administrative authentication information (e.g., user id/password).
- Replay attacks involving signaling.

B.2 Theft of Service:

- Unlawful taking of a benefit of a service provider intended to deprive the service provider of lawful revenue.
- Defrauding service provider.
- Unauthorized deletion or alteration of billing information.
- Device cloning.
- Circumvention of conditional access systems (CAS).
- Massive replication/dissemination of information enabling theft of service.

B.3 Invasion of Subscriber Privacy and Eavesdropping:

- Call Pattern Tracking to discover identity, affiliation, presence and usage.
- Traffic Capture - unauthorized recording of traffic including packet recording, packet logging and packet snooping. Includes mangement and signaling traffic.
- Unauthorized access to subscriber media stream.
- Unauthorized access to operations, administration, management & provisioning (OAM&P) traffic.
- Unauthorized access to signaling traffic.
- Information Harvesting - unauthorized means of capturing identity that enables subsequent unauthorized communication and theft of information. Consists of the collection of IDs, which may be numbers, strings, URLs, etc.
- Media Reconstruction - unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation, and/or feature extraction of any portion of a video communication including identity, presence or status.
- Unauthorized disclosure of subscriber service capabilities.
- Unauthorized disclosure of subscriber's previous or current usage or activities (e.g., subscriber viewing history of broadcast or VoD content, on-line gaming activities, etc.).
- Replay attacks involving media (re-playing captured media for malicious gains, or invading privacy by replaying media for personal use).

B.4 Interception & Modification:

- Conversation Impersonation & Hijacking - the injection, deletion, addition, removal, substitution or replacement or other modification of any portion of a communication with information that alters any of its content and/or the identity, presence or status of any of its parties. Includes management and signaling traffic.
- Unauthorized access, modification or deletion of digital information.
- Hijack data stream; insertion, modification and deletion data stream in an unauthorized manner.
- Any form of SPAM.
- Unauthorized transmission of material (for political or other reasons).

B.5 Traffic/Packet Flooding:

- DoS attack on a user endpoint by sending a large number of valid packets causing interruption of service, some of which may impact network elements as well. Application stops due to overload.
- Endpoint packet flooding scenarios cause network element, or server to crash, reboot, or exhaust all resources.
- DOS - bandwidth consumption or resource consumption; high volume of traffic (e.g., to a multicast group).
- Potentially impacting thousands of subscribers (e.g., DSLAMs, servers that support thousands of subscribers).

B.6 Malformed Packets & Messages:

- Disabling Endpoints with Invalid Messages - DoS attack on the endpoint (e.g., server) by sending a number of invalid messages that could cause the endpoint to crash, reboot, or exhaust all resources.
- Malformed Protocol Messages - sending of malformed protocol messages (e.g., messages with overflow or underflow) to the device that degrades its performance to the point of being unable to process normal messages.
- Malformed messages that cause buffer overflow.
- Potentially impacting thousands of subscribers (e.g., servers that support thousands of subscribers).

B.7 Spoofed Messages:

- DoS attack that disrupts service by causing a session to end prematurely.
- Spoofing of control messages. Malicious control traffic - injected into the communications causing applications or servers to malfunction or traffic sent to the wrong destination. Forged control messages used to alter the structure of multicast distribution trees and affect the data distribution across them. DOS - bogus broadcast message claiming there is a high loss rate on the channel or high congestion; source will reduce the transmission rate affecting other subscriber.
- Forged end-use messages and application or server responses.
- Change IP and MAC addresses to spoof other users MAC and IP address to capture data streams.

B.8 Underlying Platform DoS:

- Vulnerabilities of the underlying operating system or firmware that the application or service runs on.
- "Point-and-shoot" exploits freely available for download on the Internet.
- DoS attacks which reduce the device's performance.
  Exploitation of these vulnerabilites has the potential to propagate to thousands of devices (e.g., client devices). Potentially resuting in redeployment of or maintenance to thousands of devices.

B.9 Compromise of Installed Software, Service-Related Data, or System Configuration:

- Malware, spyware, rootkit insertion.
- Unauthorized duplication, installation, alteration of deletion of production software and configuration files.
- Unauthorized duplication, disclosure, creation, modification, or deletion of service-related data (e.g., system logs, billing information, decryption keys, storage containers for decryption keys, etc.).
- D-DoS using compromised devices to crash the service.
- Unauthorized creation or modification of subscriber service-related information (e.g., authentication info, session keys).
- Unauthorized or unnecessary activation/deactivation of logical (protocol) ports.

B.10 Resource Exhaustion:

- Deficiencies in software or hardware that cause depletion of memory resource (e.g., buffers) in a system.
- Deficiencies in software or hardware that consumes most of CPU resources in a system.
- Hardware or software errors that limit available bandwidth of a communication link.
- Deficiencies in software or hardware that generate unnecessary messages reducing bandwidth resources.
- E.g., infinite software loops, routing loops.

B.11 Unauthorized Network Scans and Probes:

- Port scanning/ping sweeps. Attacker can run publicly available scanning software on host that has connectivity to the network. Host services on devices monitoring the ports will respond, potentially providing information to the attacker.
- Vulnerability scanning (e.g., nessus), network mapping (e.g., NMAP). Attacker can run publicly available software on host that has connectivity to the network that queries the device configuration and network topology.
- Unauthorized remote access to software or functions resident on the device (e.g., utilizing a rootkit to provide a backdoor).

B.12 Compromise of Subscriber Application Data:

- Unauthorized disclosure, creation, modification, duplication, deletion of data created and/or used by subscriber-accessible applications.
- Includes information stored in the Service Provider's network on behalf of subscribers (e.g., video content recorded by nDVR).

B.13 Theft of Content:

- Capturing digital certificate to order content and even broadcast/redistribute the stream to other subscribers.
- Packet capture on home network and IP subnet.
- Output from an analog output port to an external recording device.
- Output from a digital port to an external recording device.
- Implement playing more than then number of allowed plays.
- Accessing illegitimate content (e.g., pirated content).
- Circumvention of conditional access systems (CAS).
- Copying content from disk storage on server or end-user device.

B.14 Access to Inappropriate Content:

- Accidental access.
- Deliberate access.

B.15 Compromise of Subscriber Information:

- Social engineering to obtain subscriber information.
- Unauthorized disclosure, creation, modification, duplication or deletion of subscriber information (e.g., address, phone no., account no., credit card info, DNS/ENUM entries, etc.).
- Limited to individual subscribers.

B.16 Session Hijacking and Service Masquerading:

- Impersonation of legitimate service provider. Capturing digital certificate from provider to modify streams and include any information they want.
- Impersonation of legitimate network device, video server, gaming server, DRM server.
- Man-in-the-Middle attack.
- Redirection of video stream to unauthorized device.

B.17 Unauthorized Management:

- Unauthorized use of on-board management application or execution of management commands. For example, manipulation of modem configuration to block specific services.
- Forged/modified management protocol messages. For example, manipulation of modem configuration to block or allow specific protocols (e.g., SNMP).
- Modification of remote managment messages (e.g., MITM).
- Illegitimate subscriber self-provisioning actions. For example, reconfiguring STB to remove bandwidth limitations in order to produce slow connections for other subscribers or increase bandwidth for yourself.
- Authorized management agent performing unauthorized activities.
- Unauthorized content management; e.g., loading, deleting content or modifying the trigger date (the date that content becomes available to the viewing public).
- Unauthorized subscriber management; e.g., unauthorized subscriber provisioning activities including upgrade/downgrade of subscriber viewing privileges.

ICS 35.040

Price based on 30 pages