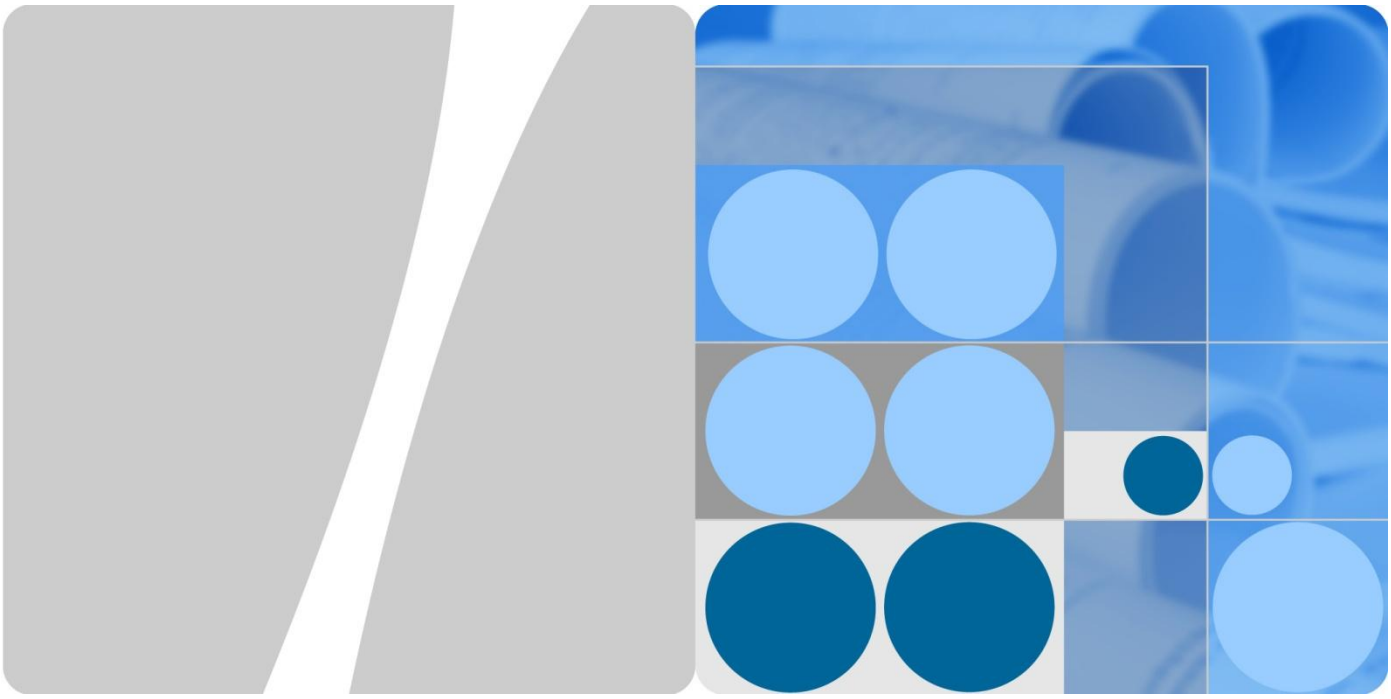


eSight V300R001C10 安全技术白皮书

文档版本 01

发布日期 2013-12-10

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

前 言

概述

本文档以 eSight ICT 统一管理系统特性和安全面临的挑战为背景，从安全策略、安全架构和产品安全性几方面详细描述了 eSight 的安全解决方案。

读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
 警告	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
 小心	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
 注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
 说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2013-12-10)

第一次正式发布。

目 录

1 简介

1.1 eSight ICT 统一管理系统概述

1.1.1 eSight ICT 统一管理系统简介

eSight 系统是华为公司研制的新一代面向企业基础网络、统一通信、智真会议、视频监控和数据中心的整体运维管理解决方案，支持对多厂商和多类型的设备进行统一的监控和配置管理，并对网络和业务质量进行监视和分析，实现对企业资源、业务、用户的统一管理以及智能联动。

1.1.2 系统特性

真正的轻量级系统，用户随时随地可访问网络，了解网络运行状态

- B/S 架构，客户端免安装，轻量化、Web 化，减轻客户端电脑载荷，减少系统维护与升级成本和工作量
- 可运行在便携机上，获得更好操作体验。

组件化管理，按需构建企业运维平台

- 统一平台，风格一致，优质的用户体验
- 按需获取，灵活选择，降低成本，避免重复投资

多厂商、多资源设备统一管理，用户可轻松实现全网设备统一管理

- 全面的设备管理能力：全面支持华为路由器、交换机、AR、安全设备、WLAN、防火墙设备、UC、存储设备的管理；预集成对 HP、Cisco、H3C 等第三方主流设备的管理能力
- 第三方设备定制能力：可支持设备厂商、设备类型、性能、告警管理的定制

全方位故障监控系统,实时了解网络故障，快速定位故障原因、排除故障

- 7*24 小时不间断的故障监控，实时的故障提醒，以及故障远程通知 故障与拓扑和设备面板之间的快速跳转
- 告警归并、告警屏蔽等措施，有效降低呈现在用户界面的告警数

可视化管理，助力用户直观了解网络状态

- 拓扑管理：提供物理拓扑和 IP 拓扑两张拓扑，实现网络设备的图形化、层次化展示，同时显示网元、链路状态
- 性能管理：多种性能监视指标，多维度呈现网络状况；性能监视视图，持续刷新；不同图表展现不同性能监视指标 以及历史数据的分析

简单便捷的日常运维操作，有效的降低运维人员的技能要求，提高工作效率

- 智能配置工具：预置了常用的业务配置模板，用户可以方便的选择模板，进行设备批量配置；通过规划表方式，进行设备差异化批量配置
- 配置文件管理：提供设备配置文件的备份、比较、恢复的功能。备份支持立即备份、周期备份、设备变更告警触发备份
- 智能报表：提供丰富的预定义报表，同时提供强大易用的报表设计功能，用户可根据行业特点和自身运维要求进行客户报表定制

高可靠的安全机制

- 通过用户分级管理、信息数据加密等方式，为系统管理数据提供了安全传输机制，保障了访问和数据安全。
- 通过对特定用户组授予特定设备的操作权限，实现分权管理，从而保障了 eSight 运行的高可靠性和安全性。

1.2 eSight 安全面临的挑战

设备层面

- 机房安全：非法进入、火灾、水灾、潮湿、雷电、静电等。
- 设备安全：盗窃、毁坏等。
- 线路安全：盗窃、窃听、干扰等。
- 介质安全：盗窃、潮湿、毁坏等。

网络层面

- 信息收集：可以用与其他类型系统相同的方法发现网络设备并对其进行剖析。通常，攻击者最初是扫描端口，识别出开放端口后，他们利用标题抓取与枚举的方法检测设备类型，并确定操作系统和应用程序的版本。具有这些信息后，攻击者可以攻击已知的可能没有更新安全补丁的缺陷。
- 嗅探：嗅探是监视网络上数据（例如明文密码或者配置信息）传输信息的行为。利用简单的数据包探测器，攻击者可以很轻松地读取所有的明文传输信息。同时，攻击者可以破解用轻量级散列算法加密的数据包，并解密您认为是安全的有用负荷。
- 欺骗：欺骗是一种隐藏某人在网上真实身份的方式。为创建一个欺骗身份，攻击者要使用一个伪造的源地址，该地址不代表数据包的真实地址。可以使用欺骗来隐藏最初的攻击源，或者绕开存在的网络访问控制列表（ACL，它根据源地址规则限制主机访问）。
- 拒绝服务（DoS/DDoS）：拒绝服务就是拒绝合法用户访问服务器或者服务。

系统层面

- 病毒、特洛伊木马和蠕虫：病毒是一种设计的程序，它进行恶意的行为，破坏操作系统或者应用程序。除了将恶意的代码包含在表面上是无害的数据文件或者可执行程序中，特洛伊木马很像一种病毒。除了可以从一个服务器自我复制到另一个服务器，蠕虫类似于特洛伊木马。蠕虫很难检测到，因为它们不是定期创建可以看见的文件。通常只有当它们开始消耗系统资源时，才能注意到它们，因为这时系统运行缓慢或者其他执行的程序停止运行。
- 足迹：足迹的示例有端口扫描、ping 扫描和 NetBIOS 枚举，它可以被攻击者用来收集系统级的有价值信息，有助于准备更严重的攻击。足迹揭示的潜在信息类型包括帐户详细信息、操作系统和其他软件的版本、服务器的名称和数据库架构的详细信息。
- 破解口令：如果攻击者不能够与服务器建立匿名连接，他将尝试建立验证连接。为此，攻击者必须知道一个有效的用户名和口令组合。如果您使用默认的帐户名称，您就给攻击者提供了一个顺利的开端，攻击者只需要破解帐户的口令即可。使用空白或者脆弱的口令可以使攻击者的工作更为轻松。
- 拒绝服务：可以通过多种方法实现拒绝服务，针对的是基础结构中的几个目标。在主机上，攻击者可以通过强力攻击应用程序而破坏服务，或者知道应用程序在其上寄宿的服务中以及运行服务器的操作系统中存在的缺陷。
- 任意执行代码：如果攻击者可以在您的服务器上执行恶意的代码，攻击者要么会损害服务器资源，要么会更进一步攻击下游系统。如果攻击者的代码所运行的服务器进程被越权执行，任意执行代码所造成的危险将会增加。常见的缺陷时允许遍历路径和缓冲区溢出攻击的未打补丁的服务器，这种情况可能导致任意执行代码。
- 未授权访问：不足的访问控制可能允许未授权的用户访问受限制信息或者执行受限制操作。

业务与应用层面

- 输入验证：缓冲区溢出，跨站点脚本编写，SQL 注入。
- 身份验证：网络窃听，暴力破解，词典攻击，重放 cookie，盗窃凭据。
- 授权：提高特权，泄漏机密数据，篡改数据，引诱攻击。
- 配置管理：未经授权访问管理接口，未经授权访问配置存储器，检索明文配置数据，越权访问配置数据。
- 敏感数据：访问存储器中的敏感数据，窃听网络，篡改数据。
- 会话管理：会话劫持；会话重放，中间人。
- 加密技术：密钥生成或密钥管理差，脆弱的或者自定义的加密术。
- 参数操作：查询字符串操作，窗体字段操作，cookie 操作，HTTP 标头操作。
- 异常处理：信息泄漏，拒绝服务。
- 安全审计：用户拒绝执行某项操作，攻击者利用没有跟踪记录的应用程序，攻击者掩饰他或者她的跟踪记录。

安全管理层面

- 缺乏安全管理规章制度，或者没有严格执行安全管理规章制度。
- 人员安全意识不足。

- 多人共用帐号，责任无法追溯。
- 安全资料不全，无法有效指导安全生产。

2 安全解决方案

2.1 安全概述

安全方案从以下三个层次来实现 eSight 系统的安全，并通过向客户提供物理层安全和管理层安全的建议，从物理和管理规则上使得整个系统提供的安全措施得以执行。

- 应用层安全解决方案：保护应用程序，如：访问控制、数据安全、通信及编码安全等。
- 系统层安全解决方案：保护操作系统、数据库、中间件及应用程序依赖的服务。
- 网络层安全解决方案：保护整个网络，为在该网络平台上运行的业务系统提供应用的支持。

2.2 安全策略

为保护 eSight 系统中的操作系统、数据库以及网络应用，引入了安全策略，这些安全策略中，大部分规则都可应用于操作系统、数据库与应用程序中。

密码管理

- 使用强密码策略与密码修改策略，如长度限制、字符组合及弱密码检测等，用于防止密码攻击。

强密码策略包括：

- 最短密码长度为 6。
- 密码中至少包括一个大写字母（A-Z）、一个小写字母（a-z）、一个数字字符（0-9）；密码中是否包含特殊字符可配置。
- 密码历史记录数可配置，取值范围是 0-30，默认为 3 个。
- 密码有效期可配置。

密码修改策略包括：

- 密码过期后强制修改密码。
- 修改自己的密码需验证旧密码。
- 重新初始化密码不受密码最短有效期的限制。

- 强制修改初始密码。
- 界面上的密码不能明文显示。
- 密码需加密保存，不允许明文保存或显示。
- 通过认证才可修改密码。
- 密码不能和用户名相同。

账号管理

- 帐号具有唯一性，帐号最短长度可配置。
- 新建帐号不能继承已删除帐号的属性。
- 锁定不在有效时间内的帐号。
- 长时间未使用自动锁定操作员帐号。
- 由系统管理员锁定的帐号只能由系统管理员手工解锁。
- 帐号锁定策略：
  - 连续登录失败锁定策略的“限定的时间段”可配置。
  - 连续登录失败锁定策略的“允许连续失败的次数”可配置。
  - 锁定时长可配置。
  - 连续登录失败锁定策略执行并在锁定时间超时后自动解锁。

权限管理

- 采用基于角色的帐号权限管理模型。
- 不能将权限直接指派到帐号。
- 新建帐号时默认最小化权限。
- 分配最小权限给运行程序的帐号。
- 分配最小权限给连接数据库的帐号。
- 纵向越权防范：对于每一个需要授权访问的 URL 请求都必须核实用户的会话标识是否合法、用户是否被授权执行这个操作。
- 横向越权防范：合理进行横向访问控制，不允许用户越权访问其他用户的敏感数据。
- 授权和用户角色数据存放在服务器端。
- 为目录和文件分配最小权限。
- 目录和文件的创建以及权限的分配自动完成。

会话管理

- 使用会话 cookie 维持会话。
- 防止会话固定。
- 会话中不允许修改的信息作为会话状态的一部分在服务器端存储和维护。
- 清除非法会话。
- 禁止使用客户端提交的未经审核的信息来给会话信息赋值。
- 用户退出清除会话信息。
- 设置会话超时机制。

- 提供“注销/退出”按钮、菜单或命令。
- 业务逻辑在服务器端处理。
- 长时间未操作锁定界面或注销用户。

认证

- eSight 系统基于会话对用户登录与鉴权进行管理，登录时引入验证码机制加强 Web 应用的安全。
- 客户端在多次连续尝试登录失败后，服务端需要进行用户帐号或者是客户端所在机器的 IP 地址的锁定策略，此锁定策略可配置。

安全协议

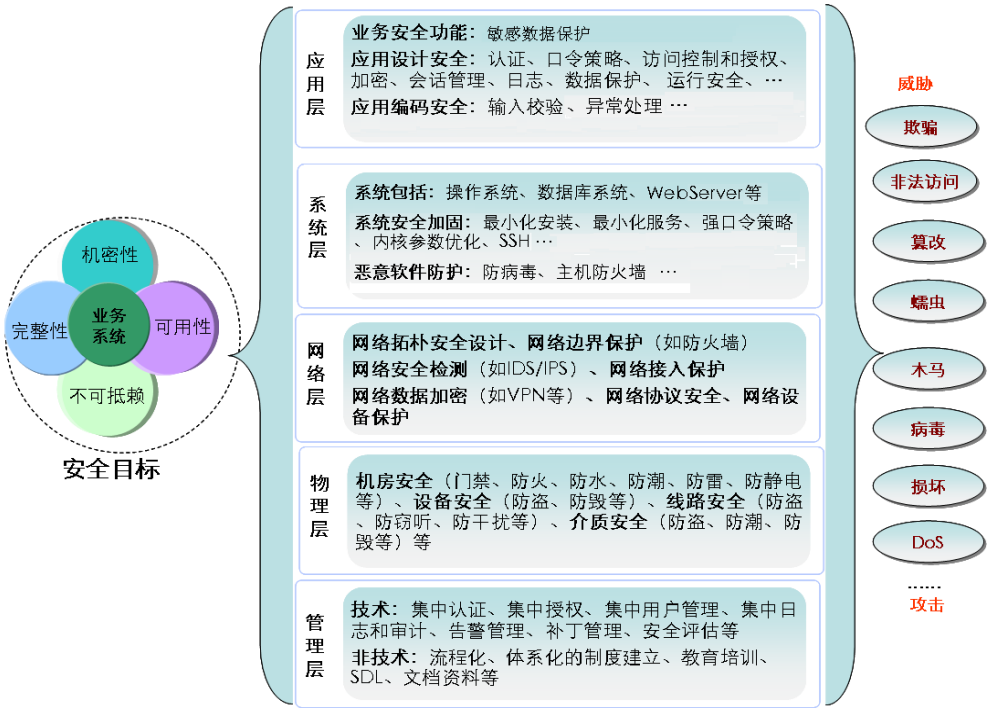
- 用户登录 eSight 时必须使用 Https（Http over SSL）协议。
- 外部用户对内部系统访问时传输的敏感数据必须使用 SSH、SFTP 等协议进行传输数据加密。
- 与设备交互使用 SSH、SNMPV3 安全协议。

安全日志

- 对安全事件及操作事件记录日志。
- 在服务器端进行日志记录。
- 安全日志必须包括的内容：事件发生的时间、客户端 IP、当前用户的标识以及对该事件的详细描述。

2.3 安全架构

eSight 产品的安全架构如下：



应用层

- 在应用层，安全方案包括认证、口令策略、访问控制与授权、加密、会话管理、日志、数据保护和运行安全等。

系统层

- 选用安全稳定的操作系统版本和数据库版本，以解决最基本的安全问题。
- 通过操作系统最小化安装，确保只安装和启用系统必须的服务，减少被黑客攻击的风险。
- 通过对操作系统加固，确保应用程序运行在安全的环境中。

网络层

- 网络管理协议使用 SNMP V2C 以上的协议版本。
- 使用 SSH V2 协议和 Https 协议，对 OS 和 eSight 进行访问和维护。
- 采用网络时间同步协议 NTP（NetWork Time Protocol）来解决确保系统内各网元保持时间的一致性。
- 提供完整的端口列表，明确标识哪些端口系统需要使用，便于用户更好地管理网络。

物理层

- 布署视频监控系统。
- 布署身份认证系统。
- 布署环境传感器。
- 如果设备提供加锁方式，将其加锁。
- 限制非授权人员进入放置鉴权设备的房间。

- 增设安全岗。

说明

物理层安全方案不包含在 eSight 系统中，用户可通过购买安防解决方案以确保 eSight 系统处在安全的物理环境中。

管理层

- 通过完好的规定和策略，定义好的过程和操作指引来避免系统弱点被攻击。
- 对管理员的管理也非常重要，这包括对管理员的职责管理及一些软措施，包括且不限于：发布一些政策、标准、过程和指引，以及提供相关的培训，监控系统的运行，改变控制过程等等。

2.4 eSight 产品安全性

2.4.1 应用层安全

帐号管理、认证与鉴权

- 采用强口令方案，对口令长度、特殊字符组合要求、密码错误次数和解锁时间等进行限制，详见“安全策略”。
- 系统中除管理员用户外的其他用户都是通过配置维护添加的，并且通过配置维护可以修改和删除。
- 操作员帐号和程序帐号等可配置为只有最小权限。
- eSight 系统基于会话对用户登录与鉴权进行管理。登录时引入验证码机制加强 Web 应用的安全。

安全日志与审计

- 管理人员对帐号的增删改操作均有记录。
- 用户登录系统、注销登录日志均有记录。
- 安全日志可用于审计。

2.4.2 系统层安全

操作系统安全

- 对操作系统进行安全加固，以保证操作系统安全。
- 通过 SSH 协议和 FTPS 协议保护系统帐号与密码不泄露。
- 通过操作系统最小化安装，确保只安装和启用系统必须的服务，减少被黑客攻击的风险。

数据库安全

- 对数据库进行安全加固，以保护数据库服务。

Web 服务安全

- 对 Tomcat 服务进行安全加固，以保证 eSight 系统运行在安全的 Web 服务之上。

日志与审计

- 操作系统与数据库可以与日志审计服务器对接，实现安全日志的集中存放与审计。
- 操作系统与日志审计服务器对接时，推荐采用 syslog 协议而不是 ftp 协议对接以保证更高的安全性。

2.4.3 网络层安全

安全通信协议

- 日常维护时，可使用 SSH 协议进行登录以保护系统数据与应用数据。
- 通过浏览器访问 eSight 系统时，登录过程采用 Https 协议以保护应用程序所使用的帐号与密码。
- 支持使用 SFTP 协议上传文件以保护系统帐号与数据安全。
- 支持使用 SNMPV3、SSH 协议访问设备。

2.4.4 物理层安全

布署监控系统

- 建议通过视频监控保护办公区域与设备房间的安全。视频监控可以在出问题后留下足够的线索与证据以分析问题所在，并对蓄意破坏的人员有威摄作用。

布署身份识别系统

- 建议对办公区域与设备房间布署身份识别系统，以对进行安全监控区域的人员进行识别。
- 限制非授权人员进入放置鉴权设备的房间以保护设备不被非授权人员直接操作。

布署传感器

- 传感器可以及时发现火灾，极大地减小火灾风险。建议布置在存放设备的房间与办公区域，以保护工作人员的生命财产安全及设备安全。

对机箱加锁

- 建议在服务器机柜或机箱提供有锁的情况下，对服务器机柜或机箱加锁，钥匙由专人管理，防止服务器被有意或无意地关机、插拔器件等。

增设安全岗

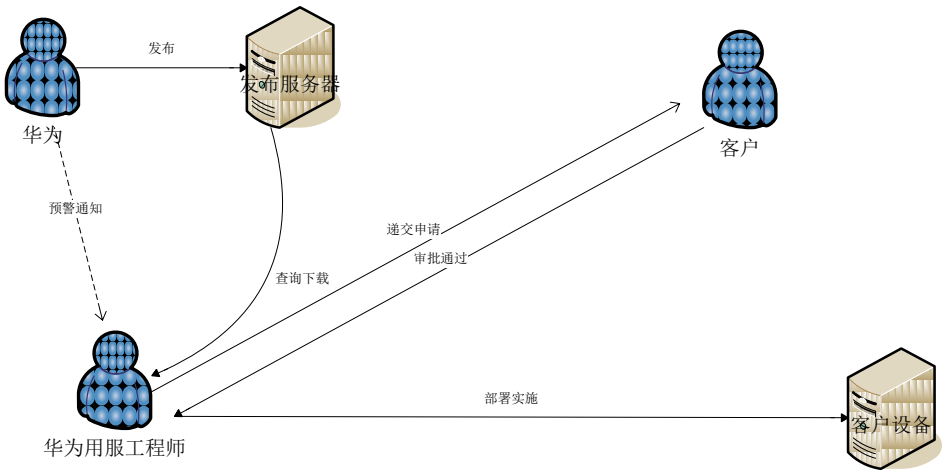
- 建议对需要进行安全控制的区域，如办公区域、生产厂区等设置安全岗，以对进入厂区的人员进行登记与监控。

2.4.5 管理层安全

补丁管理

- 制定补丁管理策略，能够支持例行和紧急情况下的补丁安装、卸载。
- 补丁管理包括操作系统、数据库和 eSight 系统等。

华为会定期发布支持的操作系统/数据库补丁列表和软件补丁，现场服务工程师通过华为预警通知或通过网站查询到后，向客户申请打补丁，客户审批通过后，由华为现场服务工程师提供打补丁服务。



组织与过程

- 建立安全管理规章制度，并严格执行安全管理规章制度。
- 对相关人员进行安全意识培训，以避免因安全意识淡薄带来的安全风险。
- 建立安全规范，并对操作人员进行培训，使安全措施得到有效的执行。
- 定期对安全日志进行检查与审计，及时发现并处理安全隐患。

帐号与权限管理

- 为每个有权限的人分配必要的权限，防止多人共用帐号，造成责任无法追溯。

3 缩略语表

术语	英文全称	中文全称
F		
FTP	File Transfer Protocol	文件传输协议。
H		
HTTP	Hyper Text Transport Protocol	超级文本传送协议
I		
ICT	Information and Communications Technology	信息和通信技术
O		
OS	Operation System	操作系统
R		
RSA	Revist-Shamir-Adleman Algorithm	RSA 加密算法。
S		
SFTP	Secure File Transfer Protocol	安全文件传输协议。
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳
SSL	Security Socket Layer	加密套接字协议层
T		
TCP	Transmission Control Protocol	传输控制协议。