税务系统信息安全等级保护基本要求

（试　行）

国家税务总局电子税务管理中心

二〇一一年八月

目　　录

引　　言

本要求根据公信安[2009]1429 号（关于印送《关于开展信息安全等级保护安全建设整改工作的指导意见》的函）对于信息安全等级保护安全建设整改工作内容的要求，以信息安全等级保护关于信息系统五个安全保护等级划分为基础，以《税务信息系统安全保障体系框架》关于税务信息系统的安全保障要求为基本内容，按照《税务系统信息安全保护层次、区域和等级划分准则》和《税务系统信息安全保护层次、区域和等级划分指南》关于信息系统安全等级的划分，参照信息安全等级保护相关国家标准，结合税务信息系统信息安全等级保护的实际进行编制。

本要求在第 1 章范围、第 2 章规范性引用文件和第 3 章术语和定义之后，第 4 章税务系统信息安全等级保护基本要求概要说明，以图示方式对税务信息系统安全等级保护基本要求的组成进行了展示，并对其组成内容进行了简要说明；第 5 章税务信息系统分等级安全技术基本要求，对第一级到第四级的税务信息系统安全等级保护的基本要求分别进行了描述。其中，5.1 节中对第一级安全技术的各项基本要求进行加粗标示，5.2 节中对第二级比第一级安全技术要求增强部分进行加粗标示，5.3 节中对第三级比第二级安全技术要求增强部分进行加粗标示，5.4 节中对第四级比第三级安全技术要求增强部分进行加粗标示；第 6 章，税务信息系统安全管理基本要求，对税务信息系统安全管理的基本要求进行了统一描述。

1 范围

本要求从安全技术和安全管理两方面规定了税务系统信息安全等级保护的基本要求，包括从第一级到第四级的各级税务信息系统的安全技术基本要求和税务信息系统安全管理基本要求。

本要求适用于各级税务单位按国家信息安全等级保护要求，进行新建税务信息系统的安全规划、设计、建设、管理和运行控制以及已投入运行信息系统的安全整改和运行控制。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB6650－86 计算机机房用活动地板技术条件

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 20269-2006 信息安全技术 信息系统安全管理要求

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 20272-2006 信息安全技术 操作系统安全技术要求

GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

GB 50174-2008 电子信息系统机房设计规范

GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求

GA/T 711-2007《信息安全技术 应用软件系统安全等级保护通用技术指南》

《税务系统信息安全保障管理与技术规范术语》

《税务系统网络与信息安全应急响应工作指南》

《税务系统网络与信息安全事件分级分类指南》

《税务系统网络与信息安全报告制度》

《税务系统网络与信息安全信息通报制度》

《税务系统网络与信息安全事件调查处理办法》

3 术语和定义

《税务系统信息安全保障管理与技术规范术语》所确立的以及以下术语和定义适用于本要求。

3.1 税务信息系统安全

税务信息系统安全保护装置的总称，由税务信息系统安全技术和税务信息系统安全管理两部分组成。税务信息系统安全技术包括组成税务信息系统的物理安全技术、主机安全技术、网络安全技术以及税务应用软件系统安全技术、数据保护安全技术、安全集中管控技术以及密码技术；税务信息系统安全管理包括安全管理机构、安全管理制度、人员安全管理、等级保护管理、安全建设管理、安全运维管理、安全变更管理、安全集中管控以及密码管理等。

3.2 税务系统信息安全

税务系统信息安全是指税务系统信息化的安全，而税务系统信息化是通过税务信息系统的建设和运行控制实现的，所以税务系统信息安全与税务信息系统安全具有基本相同的含义。

3.3 数据保护

从税务信息系统安全保护的角度，数据保护可以分为税务业务数据保护、系统重要数据保护和系统安全功能数据保护。

3.4 税务业务数据保护

是指对税务信息系统中税务业务应用处理所涉及的业务数据的保护。税务业务数据是税务信息系统所处理的税务业务的数字化表现形式，是税务信息系统安全保护的出发点和归宿。税务信息系统的安全保护归根结底都是为了确保税务业务数据的安全。

3.5 系统重要数据保护

是指对税务信息系统中实现操作系统、数据库管理系统、网络系统和应用软件系统等各类系统的功能、服务和运行控制所涉及的重要数据的保护，如系统配置表、系统资源管理表、系统运行控制表等的保护，是税务信息系统安全保护的重要内容之一。这些数据的安全性一旦受到破坏，对上述各系统的功能、服务和运行控制将会带来严重的影响。

3.6 系统安全功能数据保护

是指对实现税务信息系统各安全功能所涉及数据的保护，如鉴别信息、审计信息、主客体安全属性信息等的保护，是确保税务信息系统各安全功能模块实现其安全目标的重要保证。对税务系统安全功能数据的保护是为确保安全功能达到确定的安全目标而采取的安全保证技术措施，属于安全子系统自身安全保护的范畴。

3.7 重要设备

税务信息系统中起重要作用的设备。这些设备丢失、破坏或不能正常运行将会对税务信息系统的正常运行产生重要影响，例如：引起重要数据丢失，使信息系统的某些重要功能和服务不能按设计要求提供等。

3.8 关键设备

税务信息系统中起关键作用的设备。这些设备的丢失、破坏或不能正常运行会对税务信息系统的正常运行产生严重影响，例如：引起关键数据丢失，使信息系统的某些关键功能和服务不能按设计要求提供，甚至会使整个信息系统的运行中断。

3.9 重要局部系统

税务信息系统中可以相对独立运行的重要组成部分。当这些部分发生某些故障时，会对全系统的运行产生重要的影响。在经过对该故障进行恢复处理并恢复该局部系统运行后，可支持税务系统正常运行。

3.10 用户自我数据信息

在税务信息系统中，由用户自己创建并具有相应访问权限的数据。用户可以通过由操作系统、数据库管理系统和应用软件系统提供的操作方式，对这些数据进行响应权限所允许的操作。

3.11 税务信息系统安全集中管控

对分布在税务信息系统各个组成部分的技术和机制进行集中管理和控制。从技术角度，要求设置相应的安全技术机制，进行安全技术集中管理和控制，从管理角度，要求设置相应的安全管控岗位，配备相应的人员，实施相关的安全管控工作。

3.12 一般用户

在税务信息系统中，运行税务业务处理应用软件的用户或通过系统提供的用户操作界面对税务业务处理程序的运行进行操作控制的用户。

3.13 系统用户

在税务信息系统中，通过系统操作界面对税务信息系统的特定功能进行操作控制的用户，如系统管理员、安全员和审计员等。系统用户具有一般用户所不具有的特殊权限，所以也称特权用户。

4 税务系统信息安全等级保护基本要求概要说明

4.1 税务信息系统安全基本要求的组成

税务信息系统安全基本要求的组成如图 1 所示。

图 1 税务信息系统安全基本要求的组成

4.2 税务信息系统安全等级保护基本要求简要说明

税务系统信息安全等级保护基本要求，是根据 GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》关于各个安全等级的信息系统对于安全技术和安全管理的基本要求，参照信息安全等级保护的其他国家标准，结合税务信息系统安全保护的基本需求制定的指导税务系统安全建设和运行控制的基础性要求。本要求分别对税务信息系统从第一级到第四级的安全技术基本要求进行描述；鉴于税务系统信息安全管理的实际情况，对税务信息系统安全管理基本要求进行统一描述。

根据 GB/T22239-2008《信息安全技术 信息系统安全等级保护基本要求》的规定，本要求从物理安全技术、主机安全技术、网络安全技术、应用软件系统安全技术、数据保护技术、安全集中管控技术以及密码技术等方面，对税务信息系统安全技术基本要求进行描述。

物理安全是信息系统安全的基础，物理安全需要从组成信息系统的主机、网络的机房、设备、环境、介质等方面进行安全防护。根据 GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》关于各个安全等级的信息系统的物理安全技术基本要求，参照 GB/T 20271-2006《信息安全技术 信息系统通用安全技术要求》和 GB/T 21052-2007《信息安全

技术　信息系统物理安全技术要求》关于各个安全等级的物理安全技术要求，结合税务信息系统物理安全的实际情况，本要求从机房位置选择、机房物理访问控制、机房防雷击、机房防火、机房防水和防潮、机房防静电、机房温湿度控制、机房供配电、机房电磁防护、设备安全防护以及存储介质安全防护等方面，提出了税务信息系统第一到第四级的物理安全技术基本要求。

网络安全对税务信息系统的安全保护具有十分重要的作用。原则上，各级税务单位的各个定级系统运行于一个大的称为“税务业务专网”的网络环境。但是，实际上由网络连接的各个定级系统的组成部分（比如服务器与终端主机）需要进行保护的程度是不一样的。因此，有必要根据实际情况对整个税务业务专网按区域（子网）或网段进行划分，从实际的安全保护需要出发，对不同区域（子网）和网段实施不同安全等级的安全保护，并在其连接处实施边界保护。根据 GB/T 22239-2008《信息安全技术　信息系统安全等级保护基本要求》关于各个安全等级的信息系统的网络安全技术基本要求，参照 GB/T 20271-2006《信息安全技术 信息系统通用安全技术要求》关于各个安全等级的相关安全技术要求和 GB/T 25070-2010《信息安全技术　信息系统等级保护安全设计技术要求》关于各个安全等级信息系统的通信网络安全技术设计要求和区域边界安全设计技术要求，结合税务信息系统网络安全的实际情况，本要求从网络结构安全、网络访问控制、网络安全审计、边界完整性保护、网络入侵防范、网络恶意代码防范、网络设备登录控制以及网络备份与恢复等方面，提出了税务信息系统第一到第四级的网络安全技术基本要求。

主机是税务信息系统的重要组成部分，主机安全是税务信息系统安全的重要内容之一。在税务信息系统中，主机安全包括进行税务业务/政务处理的各类服务器、工作站以及税务内部和外部的终端主机安全，主机安全主要体现为操作系统安全和数据库管理系统安全，也称系统安全。根据 GB/T 22239-2008《信息安全技术　信息系统安全等级保护基本要求》关于各个安全等级的信息系统的主机安全技术基本要求，参照 GB/T 20271-2006《信息安全技术　信息系统通用安全技术要求》关于各个安全等级的相关安全技术的安全技术要求、GB/T 20272-2006《信息安全技术　操作系统安全技术要求》和 GB/T 20273-2006《信息安全技术 数据库管理系统安全技术要求》对于各个安全等级的操作系统和数据管理系统的安全技术要求，结合税务信息系统主机安全的实际情况，本要求从主机系统的用户身份鉴别、自主访问控制、标记与强制访问控制、安全审计、入侵防范、恶意代码防范、资源控制、可信路径、可执行程序保护和备份与恢复等方面，提出了税务信息系统第一到第四级的主机安全技术基本要求。

税务应用软件系统是实现税务业务应用处理的核心内容。从信息安全的角度，税务应用软件系统的安全保护是税务信息系统安全保护的出发点和归宿。税务应用软件系统的安全保护需要主机和网络系统提供基本的支持，同时税务应用软件系统自身所提供的安全保护机制也是税务信息系统安全的重要组成部分。根据 GB/T 22239-2008《信息安全技术　信息系统安全等级保护基本要求》关于各个安全等级的信息系统的应用安全技术基本要求，参照 GB/T 20271-2006《信息安全技术　信息系统通用安全技术要求》关于各个安全等级的相关安全技术要求、GA/T 711-2007《信息安全技术　应用软件系统安全等级保护通用技术指南》对于各个安全等级的应用软件系统的安全技术要求，结合税务应用软件系统安全的实际情况，本要求从用户身份鉴别、自主访问控制、标记与强制访问控制、安全审计、检错和容错、资源控制以及可信路径等方面，提出了税务信息系统第一到第四级的应用软件系统安全技术基本要求。

税务信息系统中的数据从安全保护的角度可以划分为税务业务数据、系统数据和系统安全功能数据。税务业务数据保护是税务信息系统安全保护的出发点和归宿；系统数据保护是税务信息系统各组成部分（主机操作系统和数据库管理系统、网络系统、应用软件系统等）

正确实现其功能的重要保证；系统安全功能数据保护是实现税务信息系统各安全功能的重要保证。对税务业务数据进行存储、传输和处理是税务信息系统的基本功能，对税务业务数据的存储、传输和处理进行安全保护无疑是税务信息系统安全的中心内容。税务业务数据的存储、传输和处理的功能是通过组成税务信息系统的各部分共同实现的。在实现这些功能的过程中，当税务业务数据受某一组成部分控制时，其安全保护的责任无疑应该由该部分承担。于是，对税务业务数据的保护便被分解为由操作系统实现的税务业务数据保护、由数据库管理系统实现的税务业务数据保护、由网络实现的税务业务数据保护和由应用软件系统实现的税务业务数据保护。对税务业务数据的安全保护与对相应的对信息系统各组成部分自身数据的安全保护以及对实现税务信息系统各安全功能的安全功能模块数据的保护，共同构成了税务信息系统数据保护的内容。根据 GB/T 22239-2008《信息安全技术　信息系统安全等级保护基本要求》关于各个安全等级数据保护的安全技术基本要求，参照 GB/T 20271-2006《信息安全技术　信息系统通用安全技术要求》关于各个安全等级的相关安全技术要求，结合税务信息系统数据安全保护的实际情况，本要求从数据完整性保护、数据保密性保护、数据交换抗抵赖、数据备份与恢复等方面，提出了第一到第四级的税务信息系统的税务业务数据保护、系统数据保护和系统安全功能数据保护的安全技术基本要求。

安全集中管控技术是税务信息系统对分散在信息系统各组成部分的信息安全技术进行集中控制和管理的重要措施。本要求从安全机制集中控制和安全数据汇集管理两方面对安全技术集中管控进行了描述。

密码技术是为税务信息系统提供完整性、保密性保护和签名、认证、抗抵赖等安全机制支持的重要技术。按国家有关密码管理部门和税务总局有关要求使用密码技术是密码技术正确使用的重要保证。本要求对密码技术的具体要求进行了简要描述。

从安全管理的角度，税务信息系统安全等级保护需要有基本的安全管理措施来保证。安全管理是一个比较宽泛的概念，可分为宏观管理和微观管理。宏观管理是指从国家法律、政策法规、规划的制定到国家各种安全机构的设置和人员的配置等方面进行的安全管理；微观管理是指围绕信息系统的安全所进行的安全管理。本要求从围绕信息系统安全的微观管理提出安全管理基本要求。按照这些安全管理要求所确定的安全管理措施，可以用来保证对税务信息系统所采用的安全技术措施达到其应具有的安全设计目标或补充安全技术的不足，使信息系统达到确定安全保护等级的安全目标。

以 GB/T 22239-2008《信息安全技术　信息系统安全等级保护基本要求》第三级对安全管理的基本要求作为基本依据，参照 GB/T20269-2006《信息安全技术　信息系统安全管理要求》第三级的要求，本要求从安全管理机构、安全管理制度、人员安全管理、等级保护管理、安全开发管理、安全运维管理、安全集中管控以及密码管理等方面，对税务信息系统安全管理基本要求进行描述。

建立安全管理机构并配备必要的安全管理人员进行安全相关事项的处理是实现税务信息系统安全管理的首要内容，本要求从安全管理机构设置、人员配备及职责、安全授权和审批、安全沟通和合作及安全审核和检查等方面，提出了税务信息系统安全管理机构的基本要求。

制定安全管理制度并按制度要求规范安全相关人员的行为是税务信息系统安全管理的重要内容之一，本要求从安全管理制度的内容、安全管理制度的制定与发布、安全管理制度的评审和修订等方面，提出了税务信息系统安全管理制度的基本要求。

信息系统是一个人机系统。信息系统功能和信息系统安全功能运行的一些重要环节，需要通过各类人员的操作和控制来实现。信息安全相关人员的管理是税务信息系统安全管理的又一重要内容。本要求从人员岗位管理、人员培训与考核管理、人员安全意识教育、外来人员访问管理等方面，提出了税务信息系统人员安全管理的基本要求。

信息安全等级保护是我国当前正在实施的信息安全制度。按照国家有关职能部门的要求进行信息安全等级保护管理是税务信息系统安全管理不可缺少的重要内容之一，本要求从定级与备案管理、等级保护测评管理、整改与报备管理等方面，提出了税务信息系统等级保护管理的基本要求。

税务信息系统安全的建设是实现税务信息系统安全的重要环节。对税务信息系统安全的建设进行安全管理是确保税务信息系统安全达到确定安全目标的重要保证。本要求从税务信息系统安全设计管理、安全产品采购使用管理、自行软件开发管理、外包软件开发管理、安全工程实施管理、安全测试验收管理、安全系统交付管理以及安全服务选择管理等方面，提出了税务信息系统安全建设管理的基本要求。

税务信息系统安全运维管理是确保税务信息系统安全功能发挥其应有作用的重要保证。本要求从运行环境管理、资产管理、存储介质管理、设备管理、安全审计管理、入侵防范管理、恶意代码防范管理、网络安全管理、主机安全管理、用户授权管理、密码管理、备份与恢复管理、安全事件处置管理以及应急响应管理等方面，提出了税务信息系统安全运维管理的基本要求。

安全变更管理是税务信息系统安全管理的重要组成部分。按照变更流程进行信息系统建设、运行期间的变更是保证系统安全目标实现的重要保证。本要求对安全变更管理的具体要求进行了简要描述。

密码管理是税务信息系统安全管理的重要组成部分。按国家有关密码管理部门和税务总局有关要求管理密码是密码技术正确使用的重要保证。本要求对密码管理的具体要求进行了简要描述。

安全集中管控，是税务信息系统安全保护的重要组成部分，既是对安全策略和安全制度进行集中管理的机构，又具有对各种分散在信息系统各组成部分的各类安全机制进行集中控制和管理、对各类安全数据进行汇集和管理的功能，以及信息系统安全事件和用户授权进行集中统一管理。本要求从安全策略统一管理、安全机制集中控制、安全制度集中管理、安全数据集中管理、安全事件集中管理、用户授权统一管理以及密码集中管理等方面，提出了税务信息系统安全集中管控的基本要求。

5 税务信息系统分等级安全技术基本要求

5.1 第一级安全技术基本要求

5.1.1 物理安全技术基本要求

5.1.1.1 机房物理访问控制

本安全级要求如下：

a) 机房出/入口应有专人负责管理；

b) 没有配置电子门禁系统的机房，对进/出机房的人员应安排专人进行鉴别、控制和记录；配置电子门禁系统的机房，应保存门禁系统的日志记录；

c) 采用监控设备将机房人员进入情况传输到值班点。

5.1.1.2 机房防雷击

本安全级要求如下：

a) 机房建筑应设置避雷装置，防雷击措施至少应包括避雷针或避雷器等；

b) 防雷装置应经国家防雷检测部门检测合格，有相关合格证明。

5.1.1.3 机房防火

本安全级要求如下：

a) 机房应设置灭火设备。

5.1.1.4 机房防水和防潮

本安全级要求如下：

a) 对穿过机房墙壁和楼板的水管应有必要的保护措施；

b) 应有防止雨水通过机房窗户、屋顶和墙壁渗透的措施。

5.1.1.5 机房温湿度控制

本安全级要求如下：

a) 机房应设置必要的温、湿度监测设施，及时了解温、湿度的变化情况；

b) 采取必要措施将机房温、湿度控制在 GB50174-2008 附录 A 对 C 级机房所要求的以下范围：

1） 机房温度：开机时应控制在 18℃-28℃，停机时应控制在 5℃-35℃；

2） 机房相对湿度：开机时应控制在 35%-75%，停机时应控制在 20%-80%。

5.1.1.6 机房供配电

本安全级要求如下：

a) 设置单独的供电线路，并配置稳压装置和过压、过流防护装置及应急照明装置；

b) 机房应提供短期备用电力供电装置（如 **UPS**），以满足系统设备在正常供电系统断电情况下短期的供电需求；短期备用电力的供电时间应不少于从正常供电系统断电到正常供电系统重新供电时间的 2 倍。

5.1.1.7 设备安全防护

本安全级要求如下：

a) 主要设备应放置在机房内；

b) 设备或主要部件应安装、固定在机柜内或机架上；

c) 主要设备和机柜、机架等应有明显且不易除去的标识，如粘贴标签或铭牌。

5.1.1.8 存储介质安全防护

本安全级要求如下：

a) 存储税务业务数据的各类介质，如纸介质、磁介质、半导体介质和光介质等，应有防丢失、被毁和受损措施；

b) 存储税务业务数据的移动存储介质，应有防恶意代码感染措施。

5.1.2 网络安全技术基本要求

5.1.2.1 网络结构安全

本安全级要求如下：

a) 保证关键网络设备的业务处理能力满足基本业务需要；

b) 保证接入网络和核心网络的带宽满足基本业务需要；

c) 绘制与当前运行情况相符的网络拓扑结构图。

5.1.2.2 网络访问控制

本安全级要求如下：

a) 在网络节点和边界设置访问控制机制，按网络访问控制策略控制用户对网络的访问；

b） 网络访问控制策略应包括：

1） 根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，允许/拒绝数据包出入；

2） 通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度为用户级和系统资源级。

5.1.2.3 网络设备登录控制

本安全级要求如下：

a） 对登录网络设备的管理员用户应进行身份标识和鉴别；

b） 身份标识：在网络管理员注册到网络设备时进行，应对用户注册信息的完整性和唯一性进行保护；

c） 身份鉴别：在网络管理员登录到网络设备时进行，采用一般口令鉴别机制，并对口令信息进行保密性和完整性保护；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和网络登录连接超时自动退出等措施

d） 应删除默认用户或修改默认用户的口令，系统无法实现的除外。

5.1.3 主机安全技术基本要求

5.1.3.1 用户身份鉴别

本安全级要求如下：

a) 对登录到操作系统和数据库管理系统的一般用户和系统管理员用户进行标识和鉴别；

b) 用户标识：在每一个用户注册到系统时，采用用户名和用户标识符进行标识，并对标识信息的唯一性和完整性进行保护；

c) 用户鉴别：在每次用户登录到系统时，采用一般性的口令鉴别机制进行鉴别，并对口令信息进行保密性和完整性保护；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连接超时自动退出等措施；

d) 重新命名系统默认账户，修改这些账户的默认口令，系统无法实现的除外。

5.1.3.2 自主访问控制

本安全级要求如下：

a） 对主机操作系统和数据库管理系统设置自主访问控制；

b） 按确定的自主访问控制策略设计访问控制功能，实现用户对其所创建客体访问权限的自主控制；

c） 访问控制主体的粒度应为用户/用户组级，客体的粒度应为文件级和数据库表级；

d） 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移；

e） 限制默认账户的访问权限；系统无法实现的除外。

5.1.3.3 入侵防范

本安全级要求如下：

a) 遵循最小安装的原则，对操作系统仅安装需要的组件和实用程序；

b） 持续跟踪厂商提供的系统升级更新补丁，在经过充分测试评估后，按正式发布的系统补丁，及时进行系统修补。

5.1.3.4 恶意代码防范

本安全级要求如下：

a） 选配满足本安全级要求的主机恶意代码防范软件；原则上所有主机均应安装恶意

代码防范软件，对由于系统不支持而未安装恶意代码防范软件的主机，应采取其他措施进行恶意代码防范；

b) 及时更新恶意代码防范软件版本和恶意代码库。

5.1.3.5 备份与恢复

本安全级要求如下：

a) 对主机重要设备设置备份；当相关设备发生故障时，用备份设备替换故障设备。

5.1.4 税务应用软件系统安全技术基本要求

5.1.4.1 用户身份鉴别

本安全级要求如下：

a) 对登录到应用软件系统的一般用户和系统管理员用户进行标识和鉴别；

b) 用户标识：在每一个用户注册到应用系统时，采用用户名和用户标识符进行标识，并对标识信息的唯一性和完整性进行保护；

c) 用户鉴别：在每次用户登录到应用软件系统时，采用一般性的口令鉴别机制进行鉴别，并对口令信息进行保密性和完整性保护；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连接超时自动退出等措施；

d) 重新命名系统默认账户，修改这些账户的默认口令；系统无法实现的除外。

5.1.4.2 自主访问控制

本级税务应用软件系统应使用 **5.1.3.2** 中所提供的操作系统和数据库管理系统的自主访问控制，分别对以文件形式和以数据库形式存储的数据实施访问控制，也可根据需要按如下要求在税务应用软件系统中设置自主访问控制：

a) 按确定的自主访问控制策略设计访问控制功能，实现用户对其所创建客体访问权限的自主控制；

b) 访问控制主体的粒度应为用户/用户组级，客体的粒度应为文件级和数据库表级；

c) 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移。

5.1.4.3 检错和容错

本安全级要求如下：

a) 在应用软件系统设置检查机制，对数据按格式进行检查，发现不符合要求的进行报警，比如，对通过人机接口输入或通过通信接口输入的数据格式或长度进行检查。

5.1.5 数据保护安全技术基本要求

5.1.5.1 数据完整性保护

本安全级要求如下：

a) 在操作系统中，采用常规的完整性校验机制，对所传输的税务业务数据、操作系统自身的重要数据及其安全功能数据的完整性检验提供支持；

b) 在数据库管理系统中，采用常规的完整性校验机制，对所传输的税务业务数据、数据库管理系统自身的重要数据及其安全功能数据的完整性检验提供支持；

c) 在网络系统中，采用常规的完整性校验机制，对所传输的税务业务数据、网络系统自身的重要数据及其安全功能数据的完整性检验提供支持；

d) 在应用软件系统中，采用常规的完整性校验机制，对所传输的税务业务数据、应用软件系统自身的重要数据及其安全功能数据的完整性检验提供支持。

5.1.5.2 数据备份与恢复

本安全级要求如下：

a) 在操作系统中，提供用户自我数据信息备份与恢复功能；由用户根据需要进行自我数据备份，并在用户数据受到破坏时，用备份数据进行恢复；

b) 在数据库管理系统中，提供用户自我数据信息备份与恢复功能；由用户根据需要进行自我数据备份，并在用户数据受到破坏时，用备份数据进行恢复；

c) 在应用软件系统中，提供用户自我数据信息备份与恢复功能；由用户根据需要进行自我数据备份，并在用户数据受到破坏时，用备份数据进行恢复；

d) 对各类备份数据每年至少进行一次抽样性恢复演练。

5.2 第二级安全技术基本要求

5.2.1 物理安全技术基本要求

5.2.1.1 机房位置选择

本安全级要求如下：

a) 机房应选择在具有防震、防风和防雨等能力的建筑内；具有符合当地抗震要求的相关证明；机房外墙壁应没有对外的窗户。否则，窗户应做密封、防水处理；

b) 机房应选在外界电磁干扰小的地方。

5.2.1.2 机房物理访问控制

本安全级要求如下：

a) 机房出/入应有专人负责管理；

b) 没有配置电子门禁系统的机房，应有专人值守，对进/出机房的人员进行鉴别、控制和记录；配置电子门禁系统的机房，应保存门禁系统的日志记录；

c) 采用监控设备将机房人员进 / 出情况传输到值班点，监控文本记录至少应保留 3 个月，监控图资料至少应保留 3 个月；

d) 进入机房的外部来访人员应经过申请和审批，对其进出时间、工作内容及带进带出的设备进行记录，并有专人陪同，且应将其活动限定在工作内容所涉及的范围之内。

5.2.1.3 机房防雷击

本安全级要求如下：

a) 机房建筑应设置避雷装置，防雷击措施至少应包括避雷针或避雷器等；

b) 防雷装置应经国家防雷检测部门检测合格，有相关合格证明；

c) 机房应设置交流电源地线。

5.2.1.4 机房防火

本安全级要求如下：

a) 机房设置的消防设施应达到 GB 50174-2008 中 B 类电子信息系统机房的消防要求；

b) 机房应设置火灾自动报警系统，并向当地公安消防部门备案。

5.2.1.5 机房防水和防潮

本安全级要求如下：

a) 对穿过机房墙壁和楼板的水管应有必要的保护措施；

b) 应有防止雨水通过机房窗户、屋顶和墙壁渗透的措施；

c) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；机房屋顶和活动地板下

铺有水管的，应采取有效防护措施；

d) 应有防止机房内水蒸气结露和地下积水转移与渗透的措施。

5.2.1.6 机房防静电

本安全级要求如下：

a) 机房关键设备应有接地防静电措施。

5.2.1.7 机房温湿度控制

本安全级要求如下：

a) 机房应设置必要的温、湿度监测设施，及时了解温、湿度的变化情况；

b) 机房应设置温、湿度自动调节装置，使机房温、湿度控制在 GB50174-2008 附录 A 对 B 级机房所要求的以下范围：

1） 机房温度：开机时应控制在 22℃-24℃，停机时应控制在 5℃-35℃；

2） 机房相对湿度：开机应控制在 40%-55%，停机时应控制在 40%-70%。

5.2.1.8 机房供配电

本安全级要求如下：

a) 应设置单独的供电线路，并配置稳压装置和过压、过流防护装置及应急照明装置；

b) 应提供短期备用电力供应（如 UPS），以满足系统设备在外部断电情况下短期的供电需求；短期备用电力的供电时间应不少于从正常供电系统断电到正常供电系统或备用供电系统重新供电时间的 2 倍；

5.2.1.9 机房电磁防护

本安全级要求如下：

a) 电源线和通信线缆应隔离铺设（比如，铺设在不同的桥架或管道），避免互相干扰。

5.2.1.10 设备安全防护

本安全级要求如下：

a) 主要设备应放置在机房内；

b) 设备和主要部件应安装、固定在机柜内或机架上；

c) 主要设备和机柜、机架等应有明显且不易除去的标识，如粘贴标签或铭牌；

d) 通信线缆应铺设在隐蔽处，例如可铺设在地下、管道或线槽中，并采取必要的防盗、防毁措施。

5.2.1.11 存储介质安全防护

本安全级要求如下：

a) 存储税务业务数据的各类介质，如纸介质、磁介质、半导体介质和光介质等，应有较严格的防丢失、被毁和受损措施；

b) 存储税务业务数据的移动存储介质，应有较严格的防恶意代码感染措施；

c) 备份税务业务数据的备份存储介质，应存放在机房以外的专门场所，并有较严格的防丢失、被毁和受损措施。

5.2.2 网络安全技术基本要求

5.2.2.1 网络结构安全

本安全级要求如下：

a) 关键网络设备的业务处理能力应具备冗余空间（至少为历史峰值的3倍），满足业务高峰期需要；

b） 保证接入网络和核心网络的带宽**满足业务高峰期需要**；
c） 绘制与当前运行情况相符的网络拓扑结构图；
d） 根据网络所涉及的税务业务部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

5.2.2.2 网络访问控制

本安全级要求如下：

a） 在网络节点和边界设置访问控制机制，按确定的网络访问控制策略控制用户对网络的访问；
b） 网络访问控制策略应包括：
1） 根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，允许/拒绝数据包出入；
2） 通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度为用户级和系统资源级；
3） 根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为用户级和网段级；
4） 网络访问控制应设定过滤规则集，并涵盖所有出入边界数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝；
5） 按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访问，控制粒度为用户级和系统资源级；
6） 应限制具有拨号访问权限的用户数量。

5.2.2.3 网络安全审计

本安全级要求如下：

a) 在网络节点和边界设置安全审计；
b) 审计内容包括网络设备运行状况、用户行为等安全相关事件；
c) 审计记录包括事件的日期和时间、用户、事件类型、事件是否成功等；
d) 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅、安全审计分析并生成审计报表等功能；
e) 提供安全审计事件报警、安全审计记录存储与保护等功能；审计记录应至少保存 6 个月；
f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；
g) 为安全审计机制集中控制和审计数据的汇集提供接口。

5.2.2.4 边界完整性保护

本安全级要求如下：

a） 能够对内部网络用户联接到外部网络的行为（比如，网络用户终端采用双网卡跨接外部网络，或采用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式连接其他外部网络）进行检查。

5.2.2.5 网络入侵防范

本安全级要求如下：

a) 在网络节点和边界设置入侵监测装置，监测端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等入侵行为；
b) 监测到入侵行为时，对入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等进

行记录、分析并报警。

5.2.2.6 网络设备登录控制

本安全级要求如下：

a) 对网络设备的管理员、审计员等进行身份标识、身份鉴别，**并对登录地址进行限制；**

b) 身份标识：在网络用户注册到设备时进行，应对注册信息的完整性及其在系统整个生存周期的唯一性进行保护；

c) 身份鉴别：在网络用户登录到设备时进行，采用**强化管理的口令或具有相应安全强度的其他机制，并对鉴别所使用的鉴别信息的保密性和完整性进行保护；**应具有登录失败处理功能，可采取结束会话、限制非法登录次数和网络登录连接超时自动退出等措施；**强化管理口令的具体要求如下：**

1） 采用数字、字母、符号的无规律混排方式；

2） 口令的长度至少应为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；

3） 如果设备口令不支持上述复杂度要求，应使用所支持的最长长度，并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d) 应删除默认用户或修改默认用户的口令，系统无法实现的除外；

e) 对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃取。

5.2.2.7 网络备份与恢复

本安全级要求如下：

a) 提供关键网络设备、通信线路的硬件备份；当相关设备或线路发生故障时，用备份设备或线路替换故障设备或线路；

b) 主备通信线路应采用不同运营商的设备；当相关设备或线路发生故障时进行主备切换，支持税务业务继续运行。

5.2.3 主机安全技术基本要求

5.2.3.1 用户身份鉴别

本安全级要求如下：

a) 对登录到操作系统和数据库管理系统的一般用户和系统用户（含系统管理员、审计员等）进行标识和鉴别；

b) 用户标识：在每一个用户注册到系统时，采用用户名和用户标识符进行标识，**并对标识信息在系统整个生存周期的唯一性和完整性进行保护；**

c) 用户鉴别：在每次用户登录系统时，采用**强化管理的口令或具有相应安全强度的其他机制进行鉴别，**并对鉴别所使用的数据信息的保密性和完整性进行保护；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连接超时自动退出等措施；**强化管理口令的具体要求如下：**

1） 采用数字、字母、符号的无规律混排方式；

2） 口令的长度至少为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；

3） 如果系统长度不支持上述口令复杂度要求，应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d) 重新命名系统默认账户，修改这些账户的默认口令，系统无法实现的除外。

5.2.3.2 自主访问控制

本安全级要求如下：

a) 对主机操作系统和数据库管理系统设置自主访问控制；
b) 按确定的自主访问控制策略设计访问控制功能，实现用户对其所创建客体访问权限的自主控制；
c) 访问控制主体的粒度应为**用户级**，客体的粒度应为文件级和数据库表级；
d) 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移；
e) 限制默认账户的访问权限，系统无法实现的除外。

5.2.3.3 安全审计

本安全级要求如下：

a) 在主机操作系统和数据库管理系统设置安全审计；
b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系的重要安全相关事件。例如：用户的添加和删除，审计功能的启动和关闭，审计策略的调整、权限变更，重要的系统操作（如用户登录、退出）等；
c) 审计记录应包括事件的日期和时间、用户名、事件类型、事件是否成功等；
d) 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅并生成安全审计报表等功能；
e) 提供安全审计事件报警、安全审计记录存储与保护等功能；审计记录应至少保存 6 个月；
f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；
g) 为安全审计机制集中控制和审计数据的汇集提供接口。

5.2.3.4 入侵防范

本安全级要求如下：

a) 遵循最小安装的原则，对操作系统仅安装需要的组件和实用程序；
b) 通过设置升级服务器等方式，持续跟踪厂商提供的系统升级更新补丁，在经过充分测试评估后，按正式发布的补丁，及时进行系统修补。

5.2.3.5 恶意代码防范

本安全级要求如下：

a) 选配满足本安全级要求的主机恶意代码防范软件；原则上所有主机均应安装恶意代码防范软件，对由于系统不支持而未安装恶意代码防范软件的主机，应采取其他措施进行恶意代码防范；
b) 及时更新恶意代码防范软件版本和恶意代码库。
c) **支持主机恶意代码防范软件的统一管理**。

5.2.3.6 资源控制

本安全级要求如下：

a) **通过设定终端接入方式、网络地址范围等限制终端登录；**
b) **根据安全策略设置登录终端的操作超时锁定；**
c) **限制单个用户对系统资源的最大或最小使用限度。**

5.2.3.7 备份与恢复

本安全级要求如下：

a) 对主机中的重要设备设置备份；当相关设备发生故障时，用备份设备替换故障设备；

b) 对主机中的重要局部系统设置备份，并定期（每月至少一次）进行备份；当相关部分发生故障时，进行局部系统恢复。

5.2.4 税务应用软件系统安全技术基本要求

5.2.4.1 用户身份鉴别

本安全级要求如下：

a) 对登录到应用软件系统的一般用户和系统用户（含系统管理员、审计员等）进行标识和鉴别；

b) 用户标识：在每一个用户注册到应用软件系统时，采用用户名和用户标识符进行标识，**并对标识信息在系统整个生存周期的唯一性和完整性进行保护；**

c) 用户鉴别：在每次用户登录应用软件系统时，采用**强化管理的口令或具有相应安全强度的其他机制进行鉴别，**并对鉴别所使用的数据信息的保密性和完整性进行保护；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连接超时自动退出等措施；**强化管理口令的具体要求如下：**

1） **采用数字、字母、符号的无规律混排方式；**

2） **口令的长度至少为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；**

3） **如果系统长度不支持上述口令复杂度要求，应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。**

d) 重新命名系统默认账户，修改这些账户的默认口令，系统无法实现的除外。

5.2.4.2 自主访问控制

本级税务应用软件系统应使用 **5.2.3.2** 中所提供的操作系统和数据库管理系统的自主访问控制，分别对以文件形式和以数据库形式存储的数据实施访问控制，也可根据需要按如下要求在税务应用软件系统中设置自主访问控制：

a） 按确定的自主访问控制策略设计访问控制功能，实现用户对其所创建客体访问权限的自主控制；

b） 访问控制主体的粒度应为**用户级**，客体的粒度应为文件级和数据库表级；

c） 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移。

5.2.4.3 安全审计

本安全级要求如下：

a) 在应用软件系统设置安全审计；

b） **审计内容应包括重要用户行为、用户源（IP 地址）、资源的异常使用和重要命令的使用等应用软件系统的重要安全相关事件，例如用户登录、用户退出、增加用户、修改用户权限等操作；**

c) 审计记录应包括事件的日期和时间、用户名、事件类型、事件是否成功等；

d) 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅并生成审计报表等功能；

e） **提供安全审计事件报警、安全审计记录存储与保护等功能；审计记录应至少保存 6 个月；**

f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；

g) 为安全审计机制集中管控和审计数据的汇集提供接口。

5.2.4.4 检错和容错

本安全级要求如下：

a) 在应用软件系统设置检查机制，对数据按格式进行检查，发现不符合要求的进行报警，比如，对通过人机接口输入或通过通信接口输入的数据格式或长度进行检查。

5.2.4.5 资源控制

本安全级要求如下：

a) **当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；**
b) **能对应用系统的最大并发会话连接数进行限制；**
c) **能对单个账户的多重并发会话连接数进行限制。**

5.2.5 数据保护安全技术基本要求

5.2.5.1 数据完整性保护

本安全级要求如下：

a) 在操作系统中，采用常规的完整性校验机制**或基于密码的完整性检验机制**，对所**存储**和传输的税务业务数据、操作系统自身的重要数据及其安全功能数据的完整性检验提供支持；**采用回退技术实现处理过程中税务业务数据的完整性保护；**
b) 在数据库管理系统中，采用常规的完整性校验机制**或基于密码的完整性检验机制**，对所**存储**和传输的税务业务数据、数据库管理系统自身的重要数据及其安全功能数据的完整性检验提供支持；**采用回退技术实现处理过程中税务业务数据的完整性保护；**
c) 在网络系统中，采用常规的完整性校验机制**或基于密码的完整性检验机制**，对所传输的税务业务数据、网络系统自身的重要数据及其安全功能数据的完整性检验提供支持；
d) 在应用软件系统中，采用常规的完整性校验机制**或基于密码的完整性检验机制**，对所传输的税务业务数据、应用软件系统自身的重要数据及其安全功能数据的完整性检验提供支持。

5.2.5.2 数据保密性保护

本安全级要求如下：

a) **在操作系统中，采用密码机制或其他具有相应强度的保密性保护机制，对所存储和传输的税务业务数据、操作系统自身的重要数据及其安全功能数据的保密性保护提供支持；对于动态管理和使用的存储重要数据信息的客体资源，在这些客体资源重新分配前，对其原使用者的数据信息进行清除；**
b) **在数据库管理系统中，采用密码机制或其他具有相应强度的保密性保护机制，对所存储和传输的税务业务数据、数据库管理系统自身的重要数据及其安全功能数据的保密性保护提供支持；对于动态管理和使用的存储重要数据信息的客体资源，在这些客体资源重新分配前，对其原使用者的数据信息进行清除；**
c) **在网络系统中，采用密码机制或其他具有相应强度的保密性保护机制，对所传输的税务业务数据、网络系统自身的重要数据及其安全功能数据的保密性保护提供支持；**
d) **在应用软件系统中，采用密码机制或其他具有相应强度的保密性保护机制，对所存储和传输的税务业务数据、应用软件系统自身的重要数据及其安全功能数据的保密性保护提供支持；对使用过的动态分配资源，在释放前将其中的剩余信息清除。**

5.2.5.3 数据备份与恢复

本安全级要求如下：

a) 在操作系统中，提供用户自我数据信息备份与恢复功能，由用户根据需要进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；**提供系统数据本地备份与恢复的功能，由系统管理员定期（至少每月一次）进行系统数据备份，当系统数据丢失或破坏后，由系统管理员用备份数据进行恢复；**

b) 在数据库管理系统中，提供用户自我数据信息备份与恢复功能，由用户根据需要进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；**提供系统数据本地备份与恢复的功能，由系统管理员定期（至少每月一次）进行系统数据备份，当系统数据丢失或破坏后，由系统管理员用备份数据进行恢复；**

c) 在应用软件系统中，提供用户自我数据信息备份与恢复功能，由用户根据需要进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；

d) 所有重要信息应每天进行备份，备份介质应场外存放；

e) 对各类备份数据每年至少进行一次抽样性恢复演练。

5.3 第三级安全技术基本要求

5.3.1 物理安全技术基本要求

5.3.1.1 机房位置选择

本安全级要求如下：

a) 机房及配套的办公场地应选择在具有防震、防风和防雨等能力的建筑内；具有符合当地抗震要求的相关证明；机房外墙壁应没有对外的窗户。否则，窗户应做密封、防水处理；

b) 机房应选在外界电磁干扰小和远离可能接收辐射信号的地方；

c) **机房应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁，避开易发生火灾和危险程度高的地区，避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域，避开低洼、潮湿及落雷区域，避开强震动源和强噪声源区域，避开有地震、水灾危害的区域；**

d) 机房场地设在高层建筑物上层的，应对设备采取有效固定措施。

5.3.1.2 机房物理访问控制

本安全级要求如下：

a) 机房出/入应有专人负责管理；

b) 没有配置电子门禁系统的机房，应有专人值守，对进/出机房的人员进行鉴别、控制和记录；配置电子门禁系统的机房，应保存门禁系统的日志记录；**机房应设紧急出口，供紧急情况时使用；**

c) 采用监控设备将机房人员进／出情况传输到值班点，监控记录至少应保留 3 个月；

d) 进入机房的外部来访人员应经过申请和审批，对其进出时间、工作内容及带进带出的设备进行记录，并有专人陪同，且应将其活动限定在工作内容所涉及的范围之内；

e) **机房应按管理要求划分区域进行管理，区域之间设置物理隔离装置，并在重要区域入／出口配置电子门禁系统；**

f) 机房重要区域（主机房、辅助区、支持区等）应配置电子门禁系统，控制、鉴别和记录进入的人员；重要区域前应设置交付或安装等过渡区域，用于设备的交付或安装。

5.3.1.3 机房防雷击

本安全级要求如下：

a) 机房建筑应设置避雷装置，防雷击措施至少应包括避雷针或避雷器等；

b） 防雷装置应经国家防雷检测部门检测合格，有相关合格证明；
c） 机房应设置交流电源地线；
d） **机房设置应设防雷保安装置，防止感应雷。**

5.3.1.4 机房防火

本安全级要求如下：

a） 机房设置的消防设施**应达到 GB 50174-2008 中 A 类电子信息系统机房的消防要求；**
b） 机房应设置**火灾自动报警系统，自动检测火情、自动报警、自动灭火，**并向当地公安消防部门备案；
c） **机房及相关的工作房间应采用耐火建筑材料，耐火建筑材料应达到 GB50016-2006 二级耐火等级；**
d） **机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。**

5.3.1.5 机房防水和防潮

本安全级要求如下：

a） 对穿过机房墙壁和楼板的水管应有必要的保护措施；
b） 应有防止雨水通过机房窗户、屋顶和墙壁渗透的措施；
c） 与机房设备无关的水管不得穿过机房屋顶和活动地板下；机房屋顶和活动地板下铺有水管的，应采取有效防护措施；
d） 应有防止机房内水蒸气结露和地下积水转移与渗透的措施；
e） **应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。**

5.3.1.6 机房防静电

本安全级要求如下：

a） **机房主要**设备应有接地防静电措施；
b） **机房应采用防静电活动地板；防静电活动地板应符合 GB6650－86 中 4.1 的活动地板电性能技术要求。**

5.3.1.7 机房温湿度控制

本安全级要求如下：

a） 机房应设置必要的温、湿度监测设施，及时了解温、湿度的变化情况；
b） 机房应设置温、湿度自动调节装置，使机房温、湿度控制在 GB50174-2008 附录 A 对 B 级机房所要求的以下的变化在以下范围：
1） 机房温度：开机时应控制在 22℃-24℃，停机时应控制在 5℃-35℃；
2） 机房相对湿度：开机时应控制在 40%-55%，停机时应控制在 40%-70%。

5.3.1.8 机房供配电

本安全级要求如下：

a） 应设置单独的供电线路，并配置稳压装置和过压、过流防护装置及应急照明装置；
b） 应提供短期备用电力供应（如 UPS），以满足系统设备在外部断电情况下短期的供电需求；短期备用电力的供电时间应不少于从正常供电系统断电到正常供电系统或备用供电系统启动时间的 2 倍；
c） **机房应有较长时间备用供电系统（如自备或租用发电机），以满足较长时间外部断电时系统的供电需求；**
d） **机房应设置冗余或并行的供电线路。**

5.3.1.9 机房电磁防护

本安全级要求如下：

a) 电源线和通信线缆应隔离铺设（比如，铺设在不同的桥架或管道），避免互相干扰；

b) **应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；机房或机房所在的大楼应有接地措施，且接地电阻必须小于 1 欧姆；机房验收报告应提供合格的检测结果；**

c) **应对关键设备和磁介质实施电磁屏蔽。**

5.3.1.10 设备安全防护

本安全级要求如下：

a) 主要设备应放置在机房内，**并在重要部位安装防盗监控报警系统**；

b) 设备和主要部件应安装、固定在机柜内或机架上；

c) 主要设备和机柜、机架等应有明显且不易除去的标识，如粘贴标签或铭牌；

d) 通信线缆应铺设在隐蔽处，例如可铺设在地下、管道或线槽中，并采取必要的防盗、防毁措施；

e) 应采取有效措施，发现网络通讯线路中断事件并报警。

5.3.1.11 存储介质安全防护

本安全级要求如下：

a) 存储税务业务数据的各类介质，如纸介质、磁介质、半导体介质和光介质等，应有**严格的防丢失、被毁和受损措施；**

b) 存储税务业务数据的移动存储介质，应有**严格的防恶意代码感染措施**；

c) 备份税务业务数据的备份存储介质，应存放在**机房区域之外专门设置的记录介质库**内，并有**严格的防丢失、被毁和受损措施；**

d) **记录介质的借用应规定审批权限，必要时可采用加密等方法进行保护；**

e) **对于应该删除和销毁的存有重要数据的介质，要有严格的管理和审批手续，防止被非法拷贝。**

5.3.2 网络安全技术基本要求

5.3.2.1 网络结构安全

本安全级要求如下：

a) **主要网络设备**的业务处理能力具备冗余空间（至少为历史峰值的3倍），以满足业务高峰期需要；

b) 应保证**网络各个部分的带宽**满足业务高峰期需要；

c) **业务终端与业务服务器应放置在不同的子网内，并建立安全的访问路径；**

d) 应绘制与当前运行情况相符的网络拓扑结构图；

e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f) **应避免将重要网段部署在网络边界处或直接连接外部网络系统，重要网段与其他网段之间应采取可靠的技术隔离手段；**

g) **应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；**

h) **应按照业务服务的重要性、优先级确定相关业务带宽分配原则及相应的带宽控制策略，并根据安全需求，采用网络QoS或专用带宽管理设备等措施，保证在网络发生拥堵时优先保证重要主机的带宽需要。**

5.3.2.2 网络访问控制

本安全级要求如下：

a) 在网络节点和边界设置访问控制机制，按确定的网络访问控制策略控制用户对网络资源的访问；

b) 网络访问控制策略应包括：

1) 根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，允许/拒绝数据包出入；

2) 通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度为用户级和系统资源级；

3) 根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，**控制粒度为端口级**；

4) 网络访问控制应设定过滤规则集，并涵盖所有出入边界数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝；

5) 对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；

6) 在会话处于非活跃一定时间（如超过 5 分钟）或会话结束后终止网络连接；

7) 应限制网络最大流量数及网络连接数；

8) 重要网段应采取技术手段防止地址欺骗，如通过禁用网络设备的闲置端口和采用非虚拟 IP 设备地址绑定等方式防止地址欺骗**；**

9) 限制具有拨号访问权限的用户数量；

10) 不允许通过互联网对重要信息系统进行远程维护和管理。

5.3.2.3 网络安全审计

本安全级要求如下：

a) 在网络节点和边界设置安全审计；

b) 审计内容包括网络设备运行状况、用户行为等安全相关事件；

c) 审计记录包括事件的日期和时间、用户名、事件类型、事件是否成功等；

d) 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅、**安全审计分析**并生成审计报表等功能；

e) 提供安全审计事件报警、安全审计记录存储与保护等功能；**审计记录应至少保存 6 个月；**

f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；

g) 为安全审计机制集中管控和审计数据的汇集提供接口。

5.3.2.4 边界完整性保护

本安全级要求如下：

a) 能够对非授权设备私自连接到内部网络的行为进行检查、准确定位并进行有效阻断；

b) 应能够对内部网络用户联接到外部网络的行为**（比如，**网络用户终端采用双网卡跨接外部网络，或采用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式连接其他外部网络）进行检查、**准确定位并进行有效阻断。**

5.3.2.5 网络入侵防范

本安全级要求如下：

a) 在网络节点和边界设置入侵监测装置，监测以下入侵行为：端口扫描、强力攻击、

木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

b) 监测到入侵行为时，对入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等进行记录、分析并报警；

c) 为入侵监测机制集中管控和监测信息的汇集提供接口；

d) 设置入侵监测集中管控机制，汇集和分析监测到的入侵信息，提供对入侵监测器实施远程参数设置、远程数据下载、远程启动等功能。

5.3.2.6 网络恶意代码防范

本安全级要求如下：

a) 选配满足本安全级要求的网络恶意代码防范产品；

b) 及时更新恶意代码防范软件版本和恶意代码库；

c) 具有与主机恶意代码防范软件不同的恶意代码库；

d) 支持网络恶意代码防范软件的统一管理。

5.3.2.7 网络设备登录控制

本安全级要求如下：

a) 对登录网络设备的管理员、**安全员**、审计员等进行身份标识、身份鉴别，并对登录地址进行限制；

b) 身份标识：在网络用户注册到设备时进行，应对用户注册信息的完整性及其在系统整个生存周期的其唯一性进行保护；

c) 身份鉴别：在网络用户登录到设备时进行，采用**强化管理的口令、基于生物特征、基于数字证书、其他具有相应安全强度的机制的两种或两种以上组合鉴别机制进行鉴别，并对鉴别信息进行由密码机制支持的保密性和完整性进行保护；**应具有登录失败处理功能，可采取结束会话、限制非法登录次数和网络登录连接超时自动退出等措施；强化管理口令的具体要求如下：

1） 采用数字、字母、符号的无规律混排方式；

2） 口令的长度至少应为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；

3） 如果设备口令不支持上述复杂度要求，应使用所支持的最长长度，并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d) 应删除默认用户或修改默认用户的口令，系统无法实现的除外；

e) 对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃取；不允许通过互联网对重要网络设备进行远程维护和管理。

5.3.2.8 网络备份与恢复

本安全级要求如下：

a) 提供**主要**网络设备、网络通信线路的备份；当相关设备或线路发生故障时，用备份设备或线路替换故障设备或线路；

b) 主备通信线路应采用不同运营商的设备；当相关设备或线路发生故障时进行主备**自动**切换，支持税务业务不间断运行。

5.3.3 主机安全技术基本要求

5.3.3.1 用户身份鉴别

本安全级要求如下：

a) 对登录到操作系统和数据库管理系统的一般用户和系统用户（含管理员、**安全员**、审计员等）进行标识和鉴别；

b） 用户标识：在每一个用户注册到系统时，采用用户名和用户标识符进行标识，并对标识信息在系统整个生存周期的唯一性和完整性进行保护；

c） 用户鉴别：在每次用户登录系统和重新连接系统时，采用**基于强化管理的口令、基于生物特征、基于数字证书或其他具有相应安全强度的身份鉴别机制进行用户身份鉴别，对系统用户应采用两种或两种以上组合的鉴别机制进行身份鉴别；对鉴别信息进行由密码机制或其它具有相应安全强度的安全机制支持的保密性和完整性保护**；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连接超时自动退出等措施；强化管理口令的具体要求如下：

1） 采用数字、字母、符号的无规律混排方式；

2） 口令的长度至少为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；

3） 如果系统长度不支持上述口令复杂度要求，应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d） 重新命名系统默认账户，修改这些账户的默认口令，**并及时进行更新，**系统无法实现的除外。

5.3.3.2 自主访问控制

本安全级要求如下：

a) 对主机操作系统和数据库管理系统设置自主访问控制；

b) 按确定的自主访问控制策略设计访问控制功能，实现用户对其所创建客体访问权限的自主控制；

c) 访问控制主体的粒度应为用户级，客体的粒度应为文件级、**数据库表和/或记录、字段级；**

d) 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移；

e) 限制默认账户的访问权限，系统无法实现的除外。

5.3.3.3 标记与强制访问控制

本安全级要求如下：

a) 在主机操作系统和数据库管理系统中设置强制访问控制；

b) 由安全员对强制访问控制策略所覆盖的主、客体设置敏感标记，为实现系统对这些主体访问客体的行为按策略所确定的规则进行强制性控制提供支持；

c) 按确定的强制访问控制策略设置强制访问控制功能，在访问控制策略控制范围内，按照访问控制策略所规定的访问控制规则，实现主体对客体访问的强制控制；

d) 强制访问控制主体的粒度应为用户级，客体的粒度应为文件级、数据库表和/或记录、字段级；

e) 根据系统用户的角色分配权限，实现系统用户的权限分离，仅授予系统用户为完成各自任务所需的最小权限。

5.3.3.4 安全审计

本安全级要求如下：

a) 在主机操作系统和数据库管理系统设置安全审计；

b） 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统的重要安全相关事件。例如：用户的添加和删除，审计功能的启动和关闭，审计策略的调整、权限变更，重要的系统操作（如登录、退出）等；

c） 审计记录应包括事件的日期和时间、用户名、事件类型、事件是否成功等；
d） 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅、**安全审计分析**并生成审计报表等功能；
e） 提供安全审计事件报警、安全审计记录存储与保护等功能；审计记录应至少保存 6 个月；
f） 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；
g） 为安全审计机制集中控制和审计数据的汇集提供接口。

5.3.3.5 入侵防范

本安全级要求如下：

a） 遵循最小安装的原则，对操作系统仅安装需要的组件和实用程序；
b） 通过设置升级服务器等方式，持续跟踪厂商提供的系统和第三方软件升级更新补丁，在经过充分测试评估后，按正式发布的补丁，及时进行系统修补；
c） 设置入侵监测装置，监测对主机的入侵行为，记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发现入侵事件时报警；
d) 设置入侵监测集中管理机制，汇集和分析监测到的入侵信息，提供对入侵监测装置实施远程参数设置、远程数据下载、远程启动等功能；
e) 为入侵监测机制集中管控和监测信息的汇集提供接口。

5.3.3.6 恶意代码防范

本安全级要求如下：

a） 选配满足本安全级要求的主机恶意代码防范软件；原则上所有主机均应安装恶意代码防范软件，对由于系统不支持而未安装恶意代码防范软件的主机，应采取其他措施进行恶意代码防范；
b) 及时更新恶意代码防范软件版本和恶意代码库；
c) 具有与网络恶意代码防范软件不同的恶意代码库；
d) 支持主机恶意代码防范软件的统一管理。

5.3.3.7 资源控制

本安全级要求如下：

a） 应通过设定终端接入方式、网络地址范围等限制终端登录；
b） 应根据安全策略设置登录终端的操作超时锁定；
c） 应限制单个用户对系统资源的最大或最小使用限度；
d） **应对重要服务器的CPU、硬盘、内存、网络等资源的使用情况进行监视；**
e） **应对系统的服务水平降低到预先规定的最小值（如重要服务器的CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值）进行检测和报警。**

5.3.3.8 备份与恢复

本安全级要求如下：

a) 对主机重要设备设置备份；当相关设备发生故障时，用备份设备替换故障设备；
b) 对主机重要的局部系统设置备份功能，并定期（每月至少一次）进行备份；当相关部分发生故障时，进行局部系统恢复；
c) 对主机全系统设置备份功能，并定期（每月至少一次）进行备份；当全系统发生故障中断运行时，进行全系统恢复。

5.3.4 税务应用软件系统安全技术基本要求

5.3.4.1 用户身份鉴别

本安全级要求如下：

a) 对登录到应用软件系统的一般用户和系统用户（含管理员、**安全员**、审计员等）进行标识和鉴别；

b) 用户标识：在每一个用户注册到应用软件系统时，采用用户名和用户标识符进行标识，并对标识信息在系统整个生存周期的唯一性和完整性进行保护；

c) 用户鉴别：在每次用户登录应用软件系统时，采用**基于强化管理口令、基于生物特征、基于数字证书或其他具有相应安全强度的身份鉴别机制进行身份鉴别，并对鉴别信息进行由密码机制或其它具有相应安全强度的安全机制支持的保密性和完整性保护，对系统用户应采用两种或两种以上组合的鉴别机制进行身份鉴别；**应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连接超时自动退出等措施；强化管理口令的具体要求如下：

1） 采用数字、字母、符号的无规律混排方式；

2） 口令的长度至少为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；

3） 如果系统长度不支持上述口令复杂度要求，应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d) 重新命名系统默认账户，修改这些账户的默认口令，系统无法实现的除外。

5.3.4.2 自主访问控制

本级税务应用软件系统应使用 **5.3.3.2** 中所提供的操作系统和数据库管理系统的自主访问控制，分别对以文件形式和以数据库形式存储的数据实施访问控制，也可根据需要按如下要求在税务应用软件系统中设置自主访问控制：

a） 按确定的自主访问控制策略设计访问控制功能，实现用户对其所创建客体访问权限的自主控制；

b） 访问控制主体的粒度应为用户级，客体的粒度应为**文件级、数据库表和/或记录、字段级；**

c） 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移。

5.3.4.3 标记与强制访问控制

本级税务应用软件系统应使用 5.3.3.3 中所提供的操作系统和数据库管理系统的强制访问控制，分别对以文件形式和以数据库形式存储的数据实施强制访问控制，也可根据需要按如下要求在应用软件系统中设置强制访问控制：

a) 可采用基于 PMI 的访问控制策略或基于角色的访问控制策略，为应用软件系统设置强制访问控制；

b) 由安全员对强制访问控制策略所覆盖的主、客体设置敏感标记，为系统对这些主体访问客体的行为按规则进行强制性控制提供支持；

c) 在强制访问控制策略控制范围内，按照强制访问控制策略所规定的访问控制规则实现主体对客体访问的强制控制；

d) 强制访问控制主体的粒度应为用户级，客体的粒度应为文件级、数据库表和/或记录、字段级。

5.3.4.4 安全审计

本安全级要求如下：

a) 在应用软件系统设置安全审计；
b) 审计内容应包括重要用户行为、用户源（IP 地址）、资源的异常使用和重要命令的使用等应用软件系统的重要安全相关事件，包括每个用户的关键操作，例如用户登录、用户退出、增加用户、修改用户权限等操作；
c) 审计记录应包括事件的日期和时间、用户名、事件类型、事件是否成功等；
d) 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅、**安全审计分析**并生成审计报表等功能；
e) 提供安全审计事件报警、安全审计记录存储与保护等功能；审计记录应至少保存 6 个月；
f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；
g) 为安全审计机制集中管控和审计数据的汇集提供接口。

5.3.4.5 检错和容错

本安全级要求如下：

a) 在应用软件系统设置检查机制，对数据按格式进行检查，发现不符合要求的进行报警，比如，对通过人机接口输入或通过通信接口输入的数据格式或长度进行检查；
b) 在应用软件系统设置数据处理容错机制，对软件运行中的某些错误进行容错处理，在出现相关错误时，支持应用软件系统不间断运行，比如，在数据传输中采用校验机制对传输数据进行检验，发现错误重新进行传送。

5.3.4.6 资源控制

本安全级要求如下：

a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
b) 能够对系统的最大并发会话连接数进行限制；
c) 能够对单个账户的多重并发会话连接数进行限制；
d) **能够对一个时间段内可能的并发会话连接数进行限制；**
e) **能够对一个访问账户或一个进程资源分配的最大和最小额进行限制；**
f) **能够对系统服务水平降低到预先规定的最小值进行检测和报警；**
g) **提供服务优先级设定功能，并能根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。**

5.3.5 数据保护安全技术基本要求

5.3.5.1 数据完整性保护

本安全级要求如下：

a) 在操作系统中，采用**密码机制或其它具有相应安全强度的完整性检验机制，**对所存储和传输的税务业务数据、操作系统自身的重要数据及其安全功能数据的完整性检验提供支持，**并对检出完整性受到破坏的数据进行一定恢复**；采用回退技术实现处理过程中税务业务数据的完整性保护；
b) 在数据库管理系统中，**采用密码机制或其它具有相应安全强度的完整性检验机制，**对所存储和传输的税务业务数据、数据库管理系统自身的重要数据及其安全功能数据的完整性检验提供支持，**并对检出完整性受到破坏的数据时进行一定恢复**；采用回退技术实现处理过程中税务业务数据的完整性保护；
c) 在网络系统中，采用**密码机制或其它具有相应安全强度的完整性检验机制，**对所传输的税务业务数据、网络系统自身的重要数据及其安全功能数据的完整性检验提供支持，**并对检出完整性受到破坏的数据进行一定恢复**；

d) 在应用软件系统中，采用**密码机制或其它具有相应安全强度的完整性检验机制，**对所存储和传输的税务业务数据、应用软件系统自身的重要数据及其安全功能数据的完整性检验提供支持，**并对检出完整性受到破坏的数据进行一定恢复**。

5.3.5.2 数据保密性保护

本安全级要求如下：

a) 在操作系统中，采用**密码机制或其它具有相应安全强度的保密性保护机制**，对存储和传输的税务业务数据、操作系统自身的重要数据及其安全功能数据的保密性保护提供支持；对于动态管理和使用的存储重要数据信息的客体资源，在这些客体资源重新分配前，对其原使用者的数据信息进行清除；

b) 在数据库管理系统中，采用**密码机制或其它具有相应安全强度的保密性保护机制，**对存储和传输的税务业务数据、数据库管理系统自身的重要数据及其安全功能数据的保密性保护提供支持；对于动态管理和使用的存储重要数据信息的客体资源，在这些客体资源重新分配前，对其原使用者的数据信息进行清除；

c) 在网络系统中，采用**密码机制或其它具有相应安全强度的保密性保护机制**，对传输的税务业务数据、网络系统自身的重要数据及其安全功能数据的保密性保护提供支持；

d) 在应用软件系统中，采用**密码机制或其它具有相应安全强度的保密性保护机制，**对存储和传输的税务业务数据、应用软件系统自身的重要数据及其安全功能数据的保密性保护提供支持；对使用过的动态分配资源，在释放前将其中的剩余信息清除。

5.3.5.3 数据交换抗抵赖

本安全级要求如下：

a) 在网络系统中，采用由密码技术所提供的签名验证机制，实现数据交换抗原发抵赖和抗接收抵赖功能；

b) 在应用软件系统中，采用由密码技术所提供的签名验证机制，实现数据交换抗原发抵赖和抗接收抵赖功能。

5.3.5.4 数据备份与恢复

本安全级要求如下：

a) 在操作系统中，提供用户自我数据信息备份与恢复功能，由用户定期进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；提供系统数据**异地数据备份功能，**由系统管理员定期（每月至少一次）进行系统数据的**异地备份**，当系统数据丢失或破坏后，由系统管理员用备份数据进行恢复；

b) 在数据库管理系统中，提供用户自我数据信息备份与恢复功能，由用户定期进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；**提供系统数据异地备份功能，**由系统管理员定期（每周至少一次）进行系统数据的**异地备份**，当系统数据丢失或破坏后，由系统管理员用备份数据进行恢复；

c) 在应用软件系统中，提供用户自我数据信息备份与恢复功能，由用户定期进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；

d) 所有重要信息应每天进行备份，备份介质应场外存放；

e) 对各类备份数据每半年至少进行一次抽样性恢复演练。

5.3.6 密码技术基本要求

本安全级要求如下：

a) 采用经国家密码管理局批准的密码算法或直接使用通过国家密码管理局安全审查的密码产品；
b) 凡税务总局对密码或密码产品的使用有明确要求，应按照税务总局的要求实施；
c) 密码技术应包括为主机、网络、应用软件和数据实现保密性、完整性、身份鉴别、抗抵赖等安全功能提供支持的加密、完整性检验、签名、认证、抗抵赖，以及为实现基于密码的授权管理的强制访问控制提供支持的授权管理基础设施（PMI）等。

5.3.7 安全集中管控技术基本要求

5.3.7.1 安全机制集中控制

本安全级要求如下：

a) 对分散在税务信息系统各组成部分（包括内部终端主机）需要进行集中控制的安全机制，应分别设置集中控制服务器，通过统一的控制操作接口进行集中控制；
b) 需要进行集中控制的安全机制包括：
   1） 分散在税务信息系统各组成部分，采用相同策略的用户身份鉴别机制；
   2） 分散在税务信息系统各组成部分，采用相同策略的访问控制机制；
   3） 分散在税务信息系统各组成部分的安全审计机制；
   4） 分散在税务信息系统各组成部分的入侵防范机制；
   5） 分布在税务信息系统各组成部分的恶意代码防范机制；
   6） 为税务信息系统安全提供支持的密码机制。

5.3.7.2 安全数据汇集

本安全级要求如下：

a) 对分散在税务信息系统各组成部分需要进行汇集的安全相关数据，应分别设置数据汇集服务器，通过统一的数据格式和接口进行汇集；
b) 需要进行汇集的安全相关数据包括：
   1） 分散在税务信息系统各组成部分的安全审计机制收集的安全审计数据；
   2） 分散在税务信息系统各组成部分的入侵防范机制获取的安全监测数据；
   3） 分散在税务信息系统各组成部分的恶意代码防范机制的恶意代码防范数据；
   4） 分散在税务信息系统各组成部分的备份与恢复机制的备份数据。

5.4 第四级安全技术基本要求

5.4.1 物理安全技术基本要求

5.4.1.1 机房位置选择

本安全级要求如下：

a) 机房应选择在具有防震、防风和防雨等能力的建筑内；具有符合当地抗震要求的相关证明；机房外墙壁应没有对外的窗户。否则，窗户应做密封、防水处理；
b) 机房应选在外界电磁干扰小和远离可能接收辐射信号的地方；
c) 机房应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁，避开易发生火灾和危险程度高的地区，避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域，避开低洼、潮湿及落雷区域，避开强震动源和强噪声源区域，避开有地震、水灾危害的区域；
d) 机房场地设在高层建筑物上层的，应对设备采取有效固定措施。

5.4.1.2 机房物理访问控制

本安全级要求如下：

a) 机房出/入应有专人负责管理；
b) 机房入/出口应有专人值守，并**配置电子门禁系统，**保存门禁系统的日志记，采用监控设备将机房人员进/出情况传输到值班点，对进/出机房的人员进行鉴别、控制和记录；监控记录至少应保留 3 个月；另设紧急出口，供紧急情况时使用；
c) 进入机房的外部来访人员应经过申请和审批，对其进出时间、工作内容及带进带出的设备进行记录，并有专人陪同，且应将其活动限定在工作内容所涉及的范围之内；
d) 机房应管理要求划分区域进行管理，区域之间设置物理隔离装置，并在重要区域入／出口配置电子门禁系统；
e) 机房重要区域（主机房、辅助区、支持区等）应配置电子门禁系统，控制、鉴别和记录进入的人员；重要区域前应设置交付或安装等过渡区域，用于设备的交付或安装。

5.4.1.3 机房防雷击

本安全级要求如下：

a) 机房建筑应设置避雷装置，防雷击措施至少应包括避雷针或避雷器等；
b) 防雷装置应经国家防雷检测部门检测合格，有相关合格证明；
c) 机房应设置交流电源地线；
d) 机房设置应设防雷保安装置，防止感应雷。

5.4.1.4 机房防火

本安全级要求如下：

a) 机房设置的消防设施应达到 GB 50174-2008 中 A 类电子信息系统机房的消防要求；
b) 机房应设置火灾自动报警系统，自动检测火情、自动报警、自动灭火，并向当地公安消防部门备案；
c) 机房及相关的工作房间应采用耐火建筑材料，耐火建筑材料应达到 GB50016-2006 二级耐火等级；
d) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

5.4.1.5 机房防水和防潮

本安全级要求如下：

a) 对穿过机房墙壁和楼板的水管应有必要的保护措施；
b) 应有防止雨水通过机房窗户、屋顶和墙壁渗透的措施；
c) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；机房屋顶和活动地板下铺有水管的，应采取有效防护措施；
d) 应有防止机房内水蒸气结露和地下积水转移与渗透的措施；
e) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

5.4.1.6 机房防静电

本安全级要求如下：

a) **主要**设备应有接地防静电措施；
b) 机房应采用防静电活动地板；防静电活动地板应符合 GB6650－86 中 4.1 的活动地板电性能技术要求；
c) **应采用静电消除器等装置，减少静电的产生。**

5.4.1.7 机房温湿度

本安全级要求如下：

a) 机房应设置必要的温、湿度监测设施，及时了解温、湿度的变化情况；

b） 机房应设置温、湿度自动调节装置，使机房温、湿度控制在 GB50174-2008 附录 A 对 A 级机房所要求的以下范围：

1）机房温度：开机时应控制在 22℃-24℃，停机时应控制在 5℃-35℃；

2）机房相对湿度：开机时应控制在 40%-55%，停机时应控制在 40%-70%。

5.4.1.8 机房供配电

本安全级要求如下：

a） 应设置单独的供电线路，并配置稳压装置和过压、过流防护装置及应急照明装置；

b） 应提供短期备用电力供应（如 UPS），以满足系统设备在外部断电情况下短期的供电需求;短期备用电力的供电时间应不少于从正常供电系统断电到正常供电系统或备用供电系统启动时间的 2 倍；

c） 机房应有备用供电系统（如自备或租用发电机），以满足较长时间外部断电时系统的供电需求；

d) 机房应设置冗余或并行的供电线路。

5.4.1.9 机房电磁防护

本安全级要求如下：

a) 电源线和通信线缆应隔离铺设（比如，铺设在不同的桥架或管道），避免互相干扰；

b) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰;机房或机房所在的大楼应有接地措施，且接地电阻必须小于 1 欧姆；机房验收报告应提供合格的检测结果；

c) 应对关键设备和磁介质实施电磁屏蔽；

d) **应对关键区域实施电磁屏蔽。**

5.4.1.10 设备安全防护

本安全级要求如下：

a） 主要设备应尽量放置在机房内，并在重要部位安装防盗监控报警系统；

b） 设备和主要部件应安装、固定在机柜内或机架上；

c） 主要设备和机柜、机架等应有明显且不易除去的标识，如粘贴标签或铭牌；

d) 通信线缆应铺设在隐蔽处，例如可铺设在地下、管道或线槽中，并采取必要的防盗、防毁措施；

e) 应采取有效措施，发现网络通讯线路中断事件并报警。

5.4.1.11 存储介质安全防护

本安全级要求如下：

a) 存储税务业务数据的各类介质，如纸介质、磁介质、半导体介质和光介质等，应有严格的防丢失、被毁和受损措施；

b) 存储税务业务数据的移动存储介质，应有严格的防恶意代码感染措施；

c) 备份税务业务数据的备份存储介质，应存放在机房区域之外专门设置的记录介质库内，并有严格的防丢失、被毁和受损措施；

d) 记录介质的借用应规定审批权限，必要时可采用加密等方法进行保护；

e) 对于应该删除和销毁的存有重要数据的介质，要有严格的管理和审批手续，防止被非法拷贝。

5.4.2 网络安全技术基本要求

5.4.2.1 网络结构安全

本安全级要求如下：

a) **网络设备**的业务处理能力具备冗余空间（至少为**历史峰值的4倍**），以满足业务高峰期需要；
b) 应保证网络各个部分的带宽满足业务高峰期需要；
c) 业务终端与业务服务器应放置在不同的子网内，并建立安全的访问路径；
d) 应绘制与当前运行情况相符的网络拓扑结构图；
e) 应根据网络所涉及的各税务业务部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
f) 应避免将重要网段部署在网络边界处或直接连接外部网络系统，重要网段与其他网段之间应采取可靠的技术隔离手段；
g) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；
h) 应按照业务服务的重要性、优先级确定相关业务带宽分配原则及相应的带宽控制策略，并根据安全需求，采用网络QoS或专用带宽管理设备等措施，保证在网络发生拥堵时优先保证重要主机的带宽需要。

5.4.2.2 网络访问控制

本安全级要求如下：

a) 在网络节点和边界设置访问控制机制，按确定的网络访问控制策略控制用户对网络资源的访问；
b) 网络访问控制策略应包括：
   1) 根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，允许/拒绝数据包出入；
   2) 通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度为用户级和系统资源级；
   3) 根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；
   4) 网络访问控制应设定过滤规则集，并涵盖所有出入边界数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝；
   5) 对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；
   6) 在会话处于非活跃一定时间（如超过 5 分钟）或会话结束后终止网络连接；
   7) 应限制网络最大流量数及网络连接数；
   8) 重要网段应采取技术手段防止地址欺骗，如通过禁用网络设备的闲置端口和采用非虚拟 IP 设备地址绑定等方式防止地址欺骗；
   9) 限制具有拨号访问权限的用户数量；
   10) 不允许通过互联网对重要信息系统进行远程维护和管理；
   11) 不允许数据带通用协议通过；
   12) 根据数据的敏感标记允许或拒绝数据通过；
   13) 不开放远程拨号访问功能。

5.4.2.3 网络安全审计

本安全级要求如下：

a) **在网络节点和边界设置安全审计机制；**
b) 审计内容包括网络设备运行状况、用户行为等安全相关事件；
c) 审计记录包括事件的日期和时间、用户名、事件类型、事件是否成功等；

d) 提供按事件进行安全审计分类、安全审计事件选择以及进行安全审计查阅、安全审计分析并生成审计报告等功能；
e) 提供安全审计事件报警、安全审计记录存储与保护等功能；**审计记录应至少保存 6 个月；**
f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；
g) 为安全审计机制集中管控和审计数据的汇集提供接口。

5.4.2.4 边界完整性保护

本安全级要求如下：

a) 能够对非授权设备私自连接到内部网络的行为进行检查、准确定位并进行有效阻断；
b) 应能够对内部网络用户联接到外部网络的行为（比如，网络用户终端采用双网卡跨接外部网络，或采用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式连接其他外部网络）进行检查、准确定位并进行有效阻断。

5.4.2.5 网络入侵防范

本安全级要求如下：

a) 在网络节点和边界设置入侵监测装置，监测端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等入侵行为；
b) 监测到入侵行为时，对入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等进行记录、分析并报警；
c) 为入侵监测机制集中管控和监测信息的汇集提供接口；
d) 设置入侵监测集中管理机制，汇集和分析监测到的入侵信息，提供对入侵监测器实施远程参数设置、远程数据下载、远程启动等功能。

5.4.2.6 网络恶意代码防范

本安全级要求如下：

a) 选配**满足本安全级要求**的网络恶意代码防范软件；如果部署了主机恶意代码检测系统，可有选择地部署网络恶意代码检测系统；
b) 及时更新恶意代码防范软件版本和恶意代码库；
c) 具有与主机恶意代码防范软件不同的恶意代码库；
d) 支持网络恶意代码防范软件的统一管理。

5.4.2.7 网络设备登录控制

本安全级要求如下：

a) 对登录网络设备的管理员、安全员、审计员等用户进行身份标识、身份鉴别，并对登录地址进行限制；
b) 身份标识：在网络用户注册到设备时进行，应对用户注册信息的完整性及其在系统整个生存周期的唯一性进行保护；
c) 身份鉴别：在网络用户登录到设备时进行，采用强化管理的口令、基于生物特征、基于数字证书、其他具有相应安全强度的机制的两种或两种以上组合鉴别机制进行鉴别，并对鉴别信息进行由密码机制支持的保密性和完整性进行保护；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和网络登录连接超时自动退出等措施；强化管理口令的具体要求如下：
   1) 采用数字、字母、符号的无规律混排方式；
   2) 口令的长度至少应为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内

不能重复；

2） 如果设备口令不支持上述复杂度要求，应使用所支持的最长长度，并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d) 应删除默认用户或修改默认用户的口令，系统无法实现的除外；

e) 对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃取；不允许通过互联网对重要网络设备进行远程维护和管理。

5.4.2.8 网络备份与恢复

本安全级要求如下：

a) 提供主要网络设备、网络通信线路的备份；当相关设备或线路发生故障时，用备份设备或线路替换故障设备或线路；

b) 主备通信线路应采用不同运营商的设备；当相关网络设备或线路发生故障时进行主备自动切换，支持税务业务不间断运行。

5.4.3 主机安全技术基本要求

5.4.3.1 用户身份鉴别

本安全级要求如下：

a) 对登录到操作系统和数据库管理系统的一般用户和系统用户（含管理员、安全员、审计员等）进行标识和鉴别；

b) 用户标识：在每一个用户注册到系统时，采用用户名和用户标识符进行标识，并对标识信息在系统整个生存周期的唯一性和完整性进行保护；

c) 用户鉴别：在每次用户登录系统**和重新连接系统时**，采用基于强化管理的口令、基于生物特征、基于数字证书等鉴别机制进行用户身份鉴别，对系统用户应采用两种或两种以上机制的组合进行身份鉴别；对鉴别信息进行由密码或其它具有相应安全强度的安全机制支持的保密性和完整性保护；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连接超时自动退出等措施；强化管理口令的具体要求如下：

1） 采用数字、字母、符号的无规律混排方式；

2） 口令的长度至少为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；

3） 如果系统长度不支持上述口令复杂度要求，应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d) 重新命名系统默认账户，修改这些账户的默认口令，并及时进行更新，系统无法实现的除外。

5.4.3.2 自主访问控制

本安全级要求如下：

a) 对主机操作系统和数据库管理系统设置自主访问控制；

b) 按确定的自主访问控制策略设计访问控制功能，实现**所有用户**对所创建客体访问权限的自主控制；

c) 访问控制主体的粒度应为用户级，客体的粒度应为文件级或数据库表和/或记录、字段级；

d) 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移；

e) 限制默认账户的访问权限，系统无法实现的除外。

5.4.3.3 标记与强制访问控制

本安全级要求如下：

a) 在主机操作系统和数据库管理系统设置强制访问控制；

b) **在全系统范围内，**由安全员按照强制访问控制策略的要求，对所涉及的主、客体设置敏感标记，为实现系统对这些主体访问客体的行为按规则进行强制性控制提供支持；

c) **在全系统范围内，**按确定的强制访问控制策略设置的强制访问控制规则，实现**所有主体对所有客体访问**的强制性控制；

d) 访问控制主体的粒度应为用户级，客体的粒度应为文件和数据库表和/或记录、字段级；

e) 根据系统用户的角色分配权限，实现系统用户的权限分离，仅授予这些用户为完成各自任务所需的最小权限。

5.4.3.4 安全审计

本安全级要求如下：

a) 在主机操作系统和数据库管理系统设置安全审计机制；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系的重要安全相关事件。例如：用户的添加和删除，审计功能的启动和关闭，审计策略的调整、权限变更，重要的系统操作（如用户登录、退出）等；

c) 审计记录应包括事件的日期和时间、用户名、事件类型、事件是否成功等；

d) 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅、安全审计分析并生成审计报表等功能；

e) 提供安全审计事件报警、安全审计记录存储与保护等功能；审计记录应至少保存 6 个月；

f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；

g) 为安全审计机制集中控制和审计数据的汇集提供接口。

5.4.3.5 入侵防范

本安全级要求如下：

a) 遵循最小安装的原则，对操作系统仅安装需要的组件和实用程序；

b) 通过设置升级服务器等方式，按正式发布的补丁对系统及时进行更新；

c) 在主机系统设置入侵监测装置，监测对重要主机的入侵行为，记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生入侵事件时报警；

d) 设置入侵监测集中控制机制，汇集并分析监测到的入侵信息，提供对入侵监测装置实施远程参数设置、远程数据下载、远程启动等功能；

e) 为入侵监测机制集中管控和监测信息的汇集提供接口。

5.4.3.6 恶意代码防范

本安全级要求如下：

a) 选配满足本安全级要求的主机恶意代码防范软件；原则上所有主机均应安装恶意代码防范软件，对由于系统不支持而未安装恶意代码防范软件的主机，应采取其他措施进行恶意代码防范；

b) 及时更新恶意代码防范软件版本和恶意代码库；

c) 具有与网络恶意代码防范软件不同的恶意代码库；

d) 支持主机恶意代码防范软件的统一管理。

5.4.3.7 资源控制

本安全级要求如下：

a） 应通过设定终端接入方式、网络地址范围等限制终端登录；
b） 应根据安全策略设置登录终端的操作超时锁定；
c） 应限制单个用户对系统资源的最大或最小使用限度；
d） 应对重要服务器的CPU、硬盘、内存、网络等资源的使用情况进行监视；
e） 应对系统的服务水平降低到预先规定的最小值（如，重要服务器的CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值）进行检测和报警。

5.4.3.8 可信路径

本项要求包括：

a） **在对用户进行身份鉴别时，应能够建立一条安全的信息传输路径；**
b） **在用户对资源进行访问时，应在被访问的资源与用户之间建立一条安全的信息传输路径。**

5.4.3.9 可执行程序保护

本安全级要求如下：

a) 在系统生成过程中，采用基于密码技术的信任链安全机制，构建从操作系统到上层应用的可执行程序信任链;
b) 在系统运行过程中，对每次调入内存执行的可执行程序的完整性检验，并在检测到其完整性受到破坏时，采取有效的恢复措施。

5.4.3.10 备份与恢复

本安全级要求如下：

a) 对主机重要设备设置备份；当相关设备发生故障时，用备份设备替换故障设备；
b) 对主机重要的局部系统设置备份功能，并定期（每月至少一次）进行备份；当相关部分发生故障时，进行局部系统恢复；
c) 对主机全系统设置备份功能，并定期（每月至少一次）进行备份；当全系统发生故障中断运行时，进行全系统恢复；
d) 对主机系统设置异地灾备中心，并制定灾难备份与恢复方案；当主机系统发生灾难性故障，在短期内无法正常运行时，将业务应用快速切换到灾备中心的替换主机系统运行，并在主机系统恢复正常运行后，将业务应用换回到原主机系统运行。

5.4.4 税务应用软件系统安全技术基本要求

5.4.4.1 用户身份鉴别

本安全级要求如下：

a) 对登录到应用软件系统的一般用户和系统用户（含管理员、安全员、审计员等）进行标识和鉴别；
b) 用户标识：在每一个用户注册到应用软件系统时，采用用户名和用户标识符进行标识，对标识信息在系统整个生存周期的唯一性和完整性进行保护；
c) 用户鉴别：在每次用户登录应用软件系统和**重新连接应用软件系统时**，采用强化管理的口令、基于生物特征、基于数字证书或其他具有相应安全强度的身份鉴别机制进行用户身份鉴别，并对鉴别信息进行由密码或其它具有相应安全强度的安全机制支持的保密性和完整性保护，对系统用户应采用两种或两种以上机制的组合进行身份鉴别；应具有登录失败处理功能，可采取结束会话、限制非法登录次数和登录连

接超时自动退出等措施；强化管理口令的具体要求如下：

1） 采用数字、字母、符号的无规律混排方式；

2） 口令的长度至少为 8 位，并且每季度至少更换 1 次，更新的口令至少 5 次内不能重复；

3） 如果系统长度不支持上述口令复杂度要求，应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。

d) 重新命名系统默认账户，修改这些账户的默认口令，并及时进行更新，系统无法实现的除外。

5.4.4.2 自主访问控制

本级税务应用软件系统应使用 **5.4.3.2** 中所提供的操作系统和数据库管理系统的自主访问控制，分别对以文件形式和以数据库形式存储的数据实施访问控制，也可根据需要按如下要求在税务应用软件系统中设置自主访问控制：

a） 按确定的自主访问控制策略设计访问控制功能，实现用户对其所创建客体访问权限的自主控制；

b） 访问控制主体的粒度应为用户级，客体的粒度应为文件级或数据库表和/或记录、字段级；

c) 按授权规则和授权转移规则，由用户确定所属客体的访问权限和权限转移。

5.4.4.3 标记与强制访问控制

本级税务应用软件系统应使用 **5.4.3.3** 中所提供的操作系统和数据库管理系统的强制访问控制，分别对以文件形式和以数据库形式存储的数据实施访问控制，也可根据需要按如下要求在应用软件系统中设置强制访问控制：

a) 采用基于 PMI 的访问控制安全策略或其他强制访问控制策略，为应用软件系统设置强制访问控制；

b) **在全系统范围内，**由安全员按照强制访问控制策略的要求，对所涉及的主、客体设置敏感标记，为系统对这些主体访问客体的行为按规则进行强制性控制提供支持；

c) **在全系统范围内，**按照强制访问控制策略所规定的访问控制规则，实现主体对客体访问的强制控制；

d) 强制访问控制主体的粒度应为用户级，客体的粒度应为文件级、数据库表和/或记录、字段级。

5.4.4.4 安全审计

本安全级要求如下：

a) 在应用软件系统设置安全审计；

b） 审计内容应包括重要用户行为、用户源（IP 地址）、资源的异常使用和重要命令的使用等应用软件系统的重要安全相关事件，例如用户登录、用户退出、增加用户、修改用户权限等操作；

c） 审计记录应包括事件的日期和时间、用户名、事件类型、事件是否成功等；

d） 提供按事件进行安全审计分类、安全审计事件选择，以及进行安全审计查阅、安全审计分析并生成审计报表等功能；

e） 提供安全审计事件报警、安全审计记录存储与保护等功能；审计记录应至少保存 6 个月；

f) 在安全审计存储区记满时，应采取相应的防止安全审计数据丢失的措施；

g) 为安全审计机制集中管控和审计数据的汇集提供接口。

5.4.4.5 检错和容错

本安全级要求如下：

a) 在应用软件系统设置检错机制，对数据按格式进行检查，发现不符合要求的进行报警并作相应处理，比如，对通过人机接口输入或通过通信接口输入的数据格式或长度进行检查；

b) 在应用软件系统设置数据处理容错机制，对软件运行中的某些错误进行容错处理，在出现相关错误时，支持应用软件系统不间断运行，比如，在数据传输中采用校验机制对传输数据进行检验，发现错误重新进行传送；

c) 在应用软件系统设置运算结果容错机制，对软件运行中的运算结果进行容错处理，在某些结果出现错误时，支持应用软件系统不间断运行，比如，采用多次运算结果比对的方式，获得正确的运算结果。

5.4.4.6 资源控制

本安全级要求如下：

a) 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 能够对系统的最大并发会话连接数进行限制；

c) 能够对单个账户的多重并发会话连接数进行限制；

d) 能够对一个时间段内可能的并发会话连接数进行限制；

e) 能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

f) 能够对系统服务水平降低到预先规定的最小值进行检测和报警；

g) 提供服务优先级设定功能，并能根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

5.4.4.7 可信路径

本项要求包括：

a) 在应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径；

b) 在用户通过应用系统对资源进行访问时，应用系统应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。

5.4.5 数据保护安全技术基本要求

5.4.5.1 数据完整性保护

本安全级要求如下：

a) 在操作系统中，采用基于密码机制或其它具有相应安全强度的完整性检验机制，对所存储和传输的税务业务数据、操作系统自身的重要数据及其安全功能数据的完整性检验提供支持，**并对检出完整性受到破坏的数据进行恢复**；采用回退技术实现处理过程中税务业务数据的完整性保护；

b) 在数据库管理系统中，采用密码机制或其它具有相应安全强度的完整性检验机制，对所存储和传输的税务业务数据、数据库管理系统自身的重要数据及其安全功能数据的完整性检验提供支持，**并对检出完整性受到破坏的数据进行恢复**；采用回退技术实现处理过程中税务业务数据的完整性保护；

c) 在网络系统中，采用密码机制或其它具有相应安全强度的完整性检验机制，对所传输的税务业务数据、网络系统自身的重要数据及其安全功能数据的完整性检验提供支持，**并对检查完整性受到破坏的数据进行恢复**；

d) 在应用软件系统中，采用密码机制或其它具有相应安全强度的完整性检验机制，对所存储和传输的税务业务数据、应用软件系统自身的重要数据及其安全功能数据的完整性检验提供支持，并**对检出完整性受到破坏的数据进行恢复**。

5.4.5.2 数据保密性保护

本安全级要求如下：

a) 在操作系统中，采用密码机制或其他具有相应强度的保密性保护机制，对存储和传输的税务业务数据、操作系统自身的重要数据及其安全功能数据的保密性保护提供支持；对于动态管理和使用的存储重要数据信息的客体资源，在这些客体资源重新分配前，对其原使用者的数据信息进行清除；

b) 在数据库管理系统中，采用密码机制或其他具有相应安全强度的保密性保护机制，对存储和传输的税务业务数据、数据库管理系统自身的重要数据及其安全功能数据的保密性保护提供支持；对于动态管理和使用的存储重要数据信息的客体资源，在这些客体资源重新分配前，对其原使用者的数据信息进行清除；

c) 在网络系统中，采用密码机制或其它具有相应安全强度的保密性保护机制，对所传输的税务业务数据、网络系统自身的重要数据及其安全功能数据的保密性保护提供支持；

d) 在应用软件系统中，采用密码机制或其他具有相应安全强度的保密性保护机制，对存储和传输的税务业务数据、应用软件系统自身的重要数据及其安全功能数据的保密性保护提供支持；对使用过的动态分配资源，在释放前将其中的剩余信息清除。

5.4.5.3 数据交换抗抵赖

本安全级要求如下：

a) 在网络系统中，采用由 PKI（如 CA 系统）所提供的签名验证机制，实现数据交换抗原发抵赖和抗接收抵赖功能；

b) 在应用软件系统中，采用由 PKI（如 CA 系统）所提供的签名验证机制，实现数据交换抗原发抵赖和抗接收抵赖功能。

5.4.5.4 数据备份与恢复

本安全级要求如下：

a) 在操作系统中，提供用户自我数据信息备份与恢复功能，由用户定期进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；提供系统数据异地备份与恢复功能，由系统管理员定期进行系统数据备份，当系统数据丢失或破坏后，由系统管理员用备份数据进行恢复；

b) 在数据库管理系统中，提供用户自我数据信息备份与恢复功能，由用户定期进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；提供系统数据异地备份与恢复功能，由系统管理员定期进行系统数据备份，当系统数据丢失或破坏后，由系统管理员用备份数据进行恢复；

c) 在应用软件系统中，提供用户自我数据信息备份与恢复功能，并制定备份与恢复操作规程；由用户定期进行自我数据备份，并在用户数据受到破坏时，由用户用备份数据进行恢复；

d) 所有重要信息应每天进行备份，备份介质应场外存放；

e) 对各类备份数据**每月**至少进行一次抽样性恢复演练。

5.4.6 密码技术基本要求

本安全级要求如下：

a) 采用经国家密码管理局批准的密码算法或使用通过国家密码管理局审查的密码产品；
b) 凡税务总局对密码或密码产品的使用有明确要求，应按照税务总局的要求实施；
c) 密码技术应采用包括基于密码技术的公钥基础设施（PKI）、密钥管理基础设施（KMI）和授权管理基础设施（PMI），分别为主机、网络、应用软件和数据的安全保护提供支持；
d) PKI为主机、网络、应用软件和数据提供加密（数字信封）、完整性检验、签名、认证、抗抵赖、信任链等支持，实现保密性、完整性、身份鉴别、抗抵赖、可执行程序保护等安全功能；
e) PMI为应用软件实现基于密码的授权管理的强制访问控制提供支持；
f) KMI为PKI和PMI提供严格的密钥管理。

5.4.7 安全集中管控技术基本要求

5.4.7.1 安全机制集中控制

本安全级要求如下：

a) 对分散在税务信息系统各组成部分（包括内部终端主机）需要进行集中控制的安全机制，应分别设置集中控制和管理服务器，通过统一的控制操作接口进行集中控制；
b) 需要进行集中控制的安全机制包括：
   1) 分散在税务信息系统各组成部分，采用相同策略的用户身份鉴别机制；
   2) 分散在税务信息系统各组成部分，采用相同策略的访问控制机制；
   3) 分散在税务信息系统各组成部分的安全审计机制；
   4) 分散在税务信息系统各组成部分的入侵防范机制；
   5) 分布在税务信息系统各组成部分的恶意代码防范机制；
   6) 为税务信息系统安全提供支持的密码机制。

5.4.7.2 安全数据汇集与管理

本安全级要求如下：

a) 对分散在税务信息系统各组成部分需要进行汇集与管理的安全相关数据，应分别设置数据汇集与管理服务器，通过统一数据格式和的接口进行汇集与管理；
a) 需要进行汇集于管理的安全相关数据包括：
   1) 分散在税务信息系统各组成部分的安全审计机制收集的安全审计数据；
   2) 分散在税务信息系统各组成部分的入侵防范机制获取的安全监测数据；
   3) 分散在税务信息系统各组成部分的恶意代码防范机制的恶意代码防范数据；
   4) 分散在税务信息系统各组成部分的备份与恢复机制的备份数据。

6 税务信息系统安全管理基本要求

6.1 安全管理机构基本要求

6.1.1 安全管理机构设置

税务系统信息安全管理机构设置基本要求如下：

a) 信息安全领导机构，包括：
   1） 税务总局设置信息安全领导小组；
   2） 税务总局设置信息安全领导小组办公室；
   3） 各省级局设置信息安全领导小组；
   4） 各省局级设置信息安全领导小组办公室。

b） 信息安全执行机构，包括：

1）税务总局设置信息系统安全集中管控机构；

2）各省级局设置信息系统安全集中管控机构；

3）各地级局设置信息系统安全管理岗位；

4）各县级局设置信息系统安全管理岗位。

6.1.2 安全管理机构人员配备及职责

税务系统信息安全管理机构人员配备及职责基本要求如下：

a） 信息安全管理领导机构人员配备及职责包括：

1）税务总局信息安全领导小组配备组长一人和成员若干人。组长一般由税务总局主管信息安全的领导担任，负责税务总局信息安全领导工作；成员则由各税务业务部门和信息技术部门主管信息安全的领导担任，在组长领导下参与税务总局信息安全领导工作；

2）税务总局信息安全领导小组办公室配备主任一人和办事人员若干人。主任一般由税务总局电子税务管理中心主任担任，在领导小组的领导下办理税务总局信息安全相关的各项事务；成员则由税务总局电子税务管理中心工作人员和各税务业务部门和信息技术部门的相关人员组成，办理所分担的信息安全事务；

3）各省级局信息安全领导小组配备组长一人和成员若干人。组长一般由该省级局主管信息安全的领导担任，负责本省级局信息安全领导工作；成员则由该省级局各税务业务部门和信息技术部门主管信息安全的领导担任，在组长领导下参与该省级局信息安全领导工作；

4）各省级局信息安全领导小组办公室配备主任一人和办事人员若干人。主任一般由该省级局电子税务管理中心主任担任，在领导小组的领导下办理本省级局信息安全相关的各项事务；成员则由该省级局电子税务管理中心工作人员和各税务业务部门和信息技术部门的相关人员组成，办理所分担的信息安全事务；

b） 信息安全管理执行机构人员配备及职责包括：

1）税务总局信息系统安全集中管控机构配备主任一人和成员若干人。主任一般由税务总局电子税务管理中心主任担任，负责组织和实施税务总局信息系统的各项信息安全管理工作；成员包括系统管理员、安全员、审计员等，由专职/兼职的信息安全工作人员担任，其基本分工是：系统管理员负责信息系统的加载、配置、生成及运行的控制操作等，安全员负责信息系统相关安全系统的加载、配置、生成及运行、备份与恢复、应急响应等的控制操作，审计员负责信息系统相关审计机制的设置、审计信息的汇集和管理等；

2）各省级局设置信息系统安全集中管控机构配备主任一人和成员若干人。主任一般由该省级局电子税务管理中心主任担任，负责组织和实施省级局信息系统的各项信息安全管理工作；成员包括系统管理员、安全员、审计员等，由专职/兼职的信息安全工作人员担任，其基本分工是：系统管理员负责信息系统的加载、配置、生成及运行的控制操作等，安全员负责信息系统相关安全系统的加载、配置、生成及运行、备份与恢复、应急响应等的控制操作，审计员负责信息系统相关审计机制的设置、审计信息的汇集和管理等；

3）各地级局设置信息系统安全管理岗位，根据实际需要配备系统管理员、安全员、审计员等，由专职/兼职的信息安全工作人员担任，其基本分工是：系统管理员负责信息系统的加载、配置、生成及运行的控制操作等，安全员负责信息系统相关安全系统的加载、配置、生成及运行、备份与恢复、应急响应等的控制操作，审计员负责信息系统相关审计机制的设置、审计信息的汇集和管理等；

4）各县级局设置的信息系统安全管理岗位，可参照地级局信息系统安全管理岗位进行人员配备。

6.1.3 安全授权和审批管理

税务系统信息安全授权和审批的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级信息安全授权和审批管理；
b) 制定安全授权和审批制度，明确安全授权审批事项、审批部门和审批人，以及对各类人员进行安全授权和审批工作的要求；
c) 对系统变更、重要操作、物理访问和系统接入等重要安全相关活动应严格按照审批程序执行，对重要活动应按程序逐级审批；
d) 定期（至少半年一次）审查安全授权和审批制度的规定，根据情况变化及时变更安全授权和审批事项、审批部门和审批人等；
e) 记录审批过程并保存审批文档。

6.1.4 安全沟通和合作管理

税务系统信息安全沟通和合作管理的基本要求如下：

a) 税务总局信息安全领导小组负责税务全系统信息安全的沟通和合作的管理，应定期（至少半年一次）或根据需要及时以各种方式组织税务系统各级安全管理相关人员沟通信息安全问题，研究处理方；。
b) 各级税务单位信息安全领导机构负责本级信息安全沟通和合作的管理；
c) 应采取有效措施加强各类安全管理人员之间、内部机构之间以及信息安全各岗位人员之间的沟通和合作，定期（至少每半年一次）或根据需要及时召开协调会议，共同协作处理信息安全问题；
d) 应加强与信息安全职能部门、电信公司、及相关单位等的沟通和合作，应按照职能部门的规定开展信息安全相关工作；
e) 应加强与信息安全产品供应商、业界专家、专业的信息安全公司和相关信息安全组织的沟通和合作；
f) 应聘请信息安全专家作为常年的安全顾问，征询信息安全相关事宜。

6.1.5 安全审核和检查管理

税务系统信息安全审核和检查的基本要求如下：

a) 税务总局信息安全管理领导小组负责税务全系统信息安全的审核和检查，应定期（至少每半年一次）组织各级税务单位信息安全管理机构对本级税务系统信息安全进行审核和检查；
b) 各级税务单位信息安全领导机构负责本级信息安全审核和检查管理；
c) 制定安全审核和安全检查制度，规范安全审核和安全检查工作，按规定开展信息安全审核和检查活动；
d) 定期（至少每半年一次）或根据需要组织对税务系统的全面安全审核和检查，包括：现有安全技术和管理措施的有效性，安全配置与安全策略的一致性，安全管理制度及执行情况等；
e) 定期（至少每半年一次）或根据需要进行常规的安全审核和检查，包括系统日常运行安全、系统漏洞、备份与恢复、应急响应等情况；
f) 制定安全审核和检查表格，汇总安全审核和检查数据，形成安全审核和检查报告，并对安全审核和检查结果进行通报/汇报。

6.2 安全管理制度基本要求

6.2.1 安全管理制度内容

税务系统信息安全管理制度内容的基本要求如下：

a) 税务系统信息安全的总体方针；
b) 税务系统信息安全总体策略、总体目标、范围和原则；
c) 税务系统信息安全保障框架；
d) 税务系统信息安全管理人员各项管理活动的规定；
e) 税务系统信息安全操作人员日常管理操作的规程。

6.2.2 安全管理制度制定与发布

税务系统信息安全管理制度制定与发布的基本要求如下：

a) 税务总局信息安全管理领导小组负责税务全系统信息安全制度的制定与发布，组织或授权专门的部门或人员负责税务全系统信息安全管理制度的制定，并由税务总局信息安全领导小组发布；
b) 各级税务单位信息安全领导机构负责本级信息安全管理制度的制定与发布，组织或授权专门的部门或人员负责该税务部门的信息安全管理制度的制定，并报上一级信息安全领导机构审批后发布；
c) 税务系统信息安全管理制度应有统一的格式，并进行版本（编号）管理；
d) 税务系统信息安全管理制度在制定过程中应组织专家和相关人员进行论证；
e) 税务系统信息安全管理制度应通过正式、有效的方式发布，注明发布范围，并对收发文进行登记管理。

6.2.3 安全管理制度的评审与修订

税务系统信息安全管理制度评审与修订的基本要求如下：

a) 各级税务单位信息安全管理制度的评审和修订，应由原制定和发布机构组织修订或经其批准实施修订，并由原发布机构对修订进行发布；
b) 每年或在发生重大变更时，对税务系统信息安全管理制度进行检查和评审，对发现的管理制度的不足或由于安全需求变化或其他原因引起的需要修改的安全管理制度进行修订；每年至少应组织一次安全管理制度体系的合理性和适用性审定；
c) 对只需进行少量修改的安全管理制度的修订，可采用追加修改单的方式发布；对需要进行较大修改的安全管理制度的修订，可采用替代方式重新发布；
d) 各级税务单位信息安全管理机构应指定专门人员负责安全管理制度的日常维护管理，收集制度执行过程中的情况和问题，为制度的评审和修改积累基本素材。

6.3 人员安全管理基本要求

6.3.1 人员岗位管理

税务系统人员岗位管理的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级安全相关人员的岗位管理；
b) 制定人员岗位管理章程，规范人员岗位管理；
c) 应对从事信息安全相关岗位工作人员的身份、背景、专业资格和资质、技术技能等进行审查和考核，并签署保密协议；
d) 对从事信息安全关键岗位的人员，应从工作两年以上的税务系统内部人员中选择，并签署岗位安全协议，每个岗位应有备岗人员；

e) 系统开发人员、系统管理人员、安全管理人员应进行岗位分离；主机系统管理员、网络管理员和应用软件系统管理员的职责可由一人承担，主机系统安全员、网络安全员和应用软件系统安全员的职责可由一人承担，主机系统审计员、网络审计员和应用软件系统审计员的职责可由一人承担，但管理员、安全员和审计员之间必须严格进行岗位分离，可以由其他职责人员兼任，但禁止一人多岗；
f) 离岗人员，应终止其对税务信息系统的所有访问权限，回收各种岗位证件、徽章、标识、钥匙及其他相关物件及与税务信息安全工作相关的软硬件设备，并签署书面保密协议，办理完离岗手续，并经所属信息安全领导机构批准，方可离开原工作岗位。

6.3.2 人员培训与考核管理

税务系统人员培训与考核管理的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级税务系统信息安全人员的培训与考核管理；
b) 制定税务系统信息安全人员培训与考核办法，详细规定税务系统信息安全人员培训与考核的内容、方法和过程；
c) 对税务系统信息安全各个岗位的人员，进行安全技能、操作规程及安全基本知识的培训与考核，每年至少一次；
d) 对税务系统信息安全关键岗位的人员，除进行岗位培训与考核外，还应进行岗位安全审查和关键岗位特定技能考核；
e) 定期或不定期对各个岗位人员的保密制度执行情况进行检查；
f) 对人员培训和考核的结果应进行记录、保存，并作为人员续用的重要依据。

6.3.3 人员安全意识教育管理

税务系统人员安全意识教育管理的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级税务系统人员的信息安全意识教育；
b) 制定税务系统人员信息安全意识教育计划，详细规定人员意识教育的内容、方法和过程；
c) 安全意识教育应包括信息安全基础知识、各类人员的安全责任和惩戒措施等；
d) 采用常规宣传、短期培训等方式，对各类人员进行安全意识教育，每年至少一次；
e) 安全意识教育应进行必要的考核（至少每年一次），并将考核结果及日常情况进行记录、保存，作为人员考核的内容之一。

6.3.4 外部人员访问管理

税务系统外部人员访问税务信息系统管理的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级税务系统外部人员访问的管理；
b) 制定税务系统外部人员访问规定，明确允许外部人员访问的区域、系统、设备、信息等，以及访问过程的具体要求；
c) 外部人员访问税务信息系统安全受控区域前，应先提出书面申请，经批准后由专人全程陪同或监督，并登记备案；
d) 税务信息系统安全的关键区域一般不应允许外部人员访问；
e) 外部人员未经许可禁止携带移动介质和便携式设备进入相关区域。

6.4 税务信息系统安全等级保护管理基本要求

6.4.1 定级和备案管理

税务系统定级和备案管理的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级税务信息系统安全等级的定级和备案管理；
b) 定级和备案管理工作在税务总局信息安全领导小组的统一组织下或根据信息安全等级保护相关职能部门的要求自行组织实施；
c) 按等级保护国家职能部门的要求，税务总局制定税务系统定级备案细则，明确定级备案工作的方法、过程和要求；
d) 按GB/T 22240-2008和税务系统定级备案细则的规定，各级税务单位对所属的每一个税务信息系统确定其安全等级，并按规定的格式以书面的形式说明确定信息系统为某个安全等级的方法和理由；
e) 各级税务单位组织税务业务部门和安全技术专家对税务信息系统定级的合理性进行审定，并报上一级主管部门的批准；
f) 各级税务单位指定专门的部门或人员负责管理定级信息系统的相关材料；
g) 各级税务单位按规定的格式将定级信息系统的相关材料报等级保护相关国家职能部门备案。

6.4.2 等级测评管理

税务信息系统安全等级测评管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统的安全等级测评管理；
b) 选择税务总局认可的具有相应资质的测评机构进行安全等级测评；
c) 对新建信息系统或确定进行安全等级整改的信息系统，应在投入运行前进行安全等级测评；
d) 对运行的信息系统，应按等级保护有关职能部门和税务总局的要求进行安全等级测评，发现不符合相应等级安全保护要求的应及时整改；
e) 在信息系统发生变更时，应进行安全等级测评，发现不符合相应等级安全保护要求的应及时整改。

6.4.3 整改和报备管理

税务系统安全等级保护整改和报备管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统安全等级保护的整改和报备管理；
b) 整改和报备管理应在税务总局信息安全领导小组的统一组织下实施或根据信息安全等级保护相关职能部门的要求自行组织实施；
c) 按等级保护国家职能部门和税务总局的要求，制定整改和报备细则，明确整改和报备工作的方法、过程和要求；
d) 按《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号），对所属税务信息系统进行整改；
e) 完成整改的信息系统应按 6.4.2 的要求进行信息系统安全等级测评，并组织税务业务部门和安全技术专家对测评结果进行审定；
f) 整改结果应报上一级主管部门确认；
g) 按规定的格式，将经审定和确认的整改结果及相关材料报等级保护相关国家职能部门备案。

6.5 税务信息系统安全建设管理基本要求

6.5.1 安全设计管理

税务信息系统安全设计管理的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级税务信息系统的安全设计管理；
b) 应根据定级阶段确定的所属税务信息系统的安全保护等级，按照税务系统信息安全相关制度规范的要求设计各自的《税务信息系统安全方案》；
c) 应组织税务业务部门和安全技术专家对《税务信息系统安全方案》进行评审，并报上一级主管部门批准。

6.5.2 安全产品采购使用管理

税务系统信息安全产品采购使用管理的基本要求如下：
a) 税务总局信息安全领导小组负责统一指导税务全系统的信息安全产品的采购和使用管理；
b) 各级税务单位信息安全领导机构负责本级税务信息系统安全产品的采购和使用管理；
c) 信息安全产品的采购和使用应符合国家的有关规定；
d) 密码产品的采购和使用应符合国家密码主管部门的要求；
e) 指定或授权专门的部门负责产品的采购；
f) 可预先对产品进行选型测试，确定产品的候选范围，并定期（至少每年一次）审查和更新候选产品名单；
g) 对重要的待选安全产品可委托专业测评机构进行专项测试，作为选择的参考。

6.5.3 软件自行开发安全管理

税务信息系统软件自行开发安全管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统的软件自行开发安全管理；
b) 制定软件开发安全管理制度，说明开发过程的安全控制方法和人员行为准则；
c) 开发人员应是通过安全审查的专职人员，开发活动应受到安全控制；
d) 开发环境应与实际运行环境物理分开，测试数据和测试结果应受到安全控制；
e) 制定代码编写安全规范，防范代码编写过程中的安全隐患；
f) 按相关制度规范要求，编制软件设计的安全相关文档（包括系统的安全设计文档和指导用户进行安全运行维护和使用的文档）；
g) 对程序资源库的修改、更新、发布应经过授权和批准，以防范安全隐患。

6.5.4 软件外包开发安全管理

税务信息系统软件外包开发安全管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统的软件外包开发安全管理；
b) 与开发商签订软件开发安全协议，说明开发过程的安全管理要求；
c) 指导或协助开发商制定软件开发的安全控制方法和人员行为准则；
d) 根据开发要求对软件质量和安全目标进行测试；
e) 在软件安装之前检测软件包中可能存在的恶意代码；
f) 开发商应提供软件设计的安全相关文档和使用指南（包括安全设计文档和指导用户进行安全运行维护和使用的文档）；
g) 开发商应提供软件源代码，并标明软件代码中存在的风险。

6.5.5 安全工程实施管理

税务信息系统安全工程实施管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统的安全工程实施管理，并明确实施过程中质量管理、风险管理、变更管理、进度管理、文档管理的责任部门和责任人；

b) 制定安全工程实施管理规定，以《税务信息系统安全方案》为依据，制定详细的安全系统工程实施方案和安全工程实施过程控制细则以及明确监督检查方法和要求；
c) 监控实施全过程，提交阶段性的质量控制报告和修正建议，保证实施过程的质量和系统建设目标的实现；
d) 制定风险管理计划，用于标识、评估、降低和监视风险，以保证实施过程活动和全部技术工作任务的成功实施；
e) 按照变更管理办法，依据审批程序，审批变更需求，监控变更过程；
f) 制定工程实施详细进度计划，明确实施过程里程碑，阶段交付成果及时间控制点，利用合理的方式保证项目进度可控；
g) 制定文档管理细则，明确实施过程应提交的各类正式文档，并保存备查。

6.5.6 安全测试验收管理

税务信息系统安全测试验收管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统的安全测试验收管理；
b) 制定安全测试验收管理规定，说明安全测试验收的控制方法和人员行为准则；
c) 委托有相应资质的第三方测试机构，根据设计方案或合同要求，制订测试方案，进行安全测试，详细记录测试结果，并形成测试报告；
d) 由指定或授权的测试验收专门管理部门，根据测试报告提出测试验收意见，连同测试报告一起报信息安全领导机构；
e) 由信息安全领导机构组织相关部门和相关人员对安全测试报告和验收意见进行审定。

6.5.7 安全系统交付管理

税务信息系统安全系统交付管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统的安全系统交付管理；
b) 制定安全系统交付管理规定，说明安全系统交付的控制方法和人员行为准则；
c) 制定详细的安全系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
d) 提供安全系统的设计文档和指导用户进行安全系统运行维护和使用的文档；
e) 对负责安全系统运行维护的技术人员进行相应的技能培训。

6.5.8 安全服务选择管理

税务信息系统安全服务选择管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级税务信息系统的安全服务选择管理；
b) 选择有相应资质的服务商承担所属税务信息系统的安全相关服务工作；
c) 根据相关服务的具体内容，与服务商签订服务安全协议，说明服务过程的安全相关要求；
d) 指导或协助服务商制定服务安全管理规定，说明安全服务的安全控制方法和人员行为准则；
e) 服务商应提供相关的技术培训和服务承诺，必要时可签订专门的培训合同；
f) 根据服务协议，对服务质量和相关安全目标进行审查，并记录存档，作为选择服务商的参考。

6.6 税务信息系统安全运维管理基本要求

6.6.1 运行环境管理

税务信息系统运行环境管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的运行环境管理；
b) 制定税务信息系统运行环境管理制度，对机房入/出、外部人员访问、进出机房的物品携带、机房设施、以及人员操作等作出规定，并指定专门部门或人员定期（至少半年一次）对相关内容进行检查；
c) 实行机房设施管理责任制，机房防雷击、防火、防水防潮、防静电、温湿度控制、供配电和电磁防护等设施，应有专人负责进行维护管理，定期（至少半年一次）进行检查，发现问题及时解决；应每季度对机房供配电、空调、UPS等设施进行维护管理并保存相关维护记录；应每年对监控报警系统、防雷、消防等装置进行检测维护并保存相关维护记录；
d) 机房应作为信息系统关键部位，机房工作人员应作为关键部位工作人员，按照6.3.1中相应条款的要求进行管理；
e) 对设置终端主机的办公环境应加强管理，规范办公环境人员行为，终端主机台面应保持整洁，不应有包含敏感信息的文档，操作人员离开座位时应将终端主机退出登录状态；不在办公区接待来访人员，工作人员调离办公室应立即交还该办公室钥匙。

6.6.2 资产管理

税务信息系统资产管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的资产管理；
b) 建立资产管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
c) 编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等；
d) 对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理；
e) 根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。

6.6.3 存储介质管理

税务信息系统存储介质管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的存储介质管理；
b) 制定税务系统存储介质管理制度，对介质的存放、传输、使用、维修和销毁等作出规定；
c) 存储介质应存放在安全的环境中，并有专人进行分类登记和标识，并采取保护措施，对需要加密存储的数据进行加密；
d) 在存储介质进行物理传递时，应对负责传输的人员、包装、交接等关键环节进行严格控制，必要时进行加密保护；
e) 存储介质的使用应采用授权管理，严格按照权限分配（借出）和使用，并进行登记；
f) 存储介质维修时，应清除其所存储的敏感信息，确保信息不被泄漏；
g) 对需要销毁的存储介质，应进行严格管理，严格审批，并有两人以上共同实施销毁；
h) 对异地存放的存储备份数据的介质，环境要求和管理方法应与本地相同。

6.6.4 设备管理

税务信息系统设备管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的设备管理；
b) 制定税务信息系统设备管理制度，对设备的选型、采购、发放、操作使用和设备状况的检查维护等作出规定；
c) 对信息系统的各种软硬件设备的选型、采购、发放和领用等进行基于申报、审批和专人负责的规范化管理，各种移动设备必须经过审批才能带离机房或办公地点；

d) 对终端主机、便携机、工作站、服务器和网络等信息系统设备的操作和使用进行规范化管理，按操作规程实现设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

e) 对信息系统的各种设备（包括主机和网络的在用设备和备份、冗余设备）的管理和维护应责任到人，指定专门的部门或人员每季度至少进行一次检查和维护；涉及税务系统以外的维修和服务应有严格的审批，维修过程应进行监督控制。

6.6.5 安全审计管理

税务信息系统安全审计管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的安全审计管理；

b) 制定税务信息系统安全审计管理制度，对安全审计机制需要审计员参与的工作作出明确规定；

c) 安全审计相关操作应由审计员按权限实施；

d) 对由安全审计技术机制汇集的审计信息按规定进行存储和保护；

e) 及时组织相关人员对汇集的安全审计信息进行分析，形成分析报告，并采取必要的应对措施。

6.6.6 入侵防范管理

税务信息系统入侵防范管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的入侵防范管理；

b) 制定税务信息系统入侵防范管理制度，对入侵防范机制需要由人工参与的工作做出明确规定；

c) 入侵防范的操作由安全员按权限实施，包括对监控信息、设备状态、恶意代码、补丁升级等进行统一管理；

d) 对入侵监测装置实施远程参数设置、远程数据下载、远程启动等功能；

e) 对由入侵防范机制收集的通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等安全相关信息进行汇集，并妥善保存；

f) 及时组织相关人员对收集的入侵监测信息进行分析，发现可疑行为，形成分析报告，并采取必要的应对措施。

6.6.7 网络安全管理

税务信息系统网络安全管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的网络安全管理；

b) 制定税务信息系统网络安全管理制度，对网络安全管理事项作出明确规定；

c) 网络安全管理由安全员按权限实施，包括按《安全员手册》进行网络安全机制配置、网络安全运行控制、网络软件升级、网络漏洞及修补等通过相关操作进行控制和管理，并对配置文件定期（至少每月一次）进行离线备份；

d) 对网络漏洞进行持续跟踪，每月至少进行一次漏洞扫描，对发现的漏洞，在应对措施经过充分论证后方可进行修补；漏洞修补前应对可能的风险进行评估和充分准备，如选择恰当时间，并做好数据备份和回退方案；漏洞修补后应进行验证测试，以保证网络系统的正常运行；

e) 网络安全审计由审计员按权限实施，包括按《审计员操作手册》对需要集中管理的网络系统和网络设备的各类审计机制进行配置，对各类审计信息进行汇集、存储、维护和分析等；

f) 应实现网络设备的最小服务配置和优化配置；至少每月和在配置变更后对网络设备的配置文件进行备份；

g) 网络的所有外部连接应得到授权和批准，并定期（至少每月一次）检查违反规定拨号上网或其他违反网络安全策略的行为；
h) 按网络安全技术机制提供的功能进行网络安全运行控制，进行各类审计信息、网络监控信息的收集维护和分析处理工作；
i) 根据厂家提供的软件版本升级和补丁，及时对网络软件进行版本升级和补丁更新，并在更新前对重要文件进行备份；
j) 应禁止未经许可的便携式和移动式设备接入网络；
k) 应严格控制对网络管理员、网络安全员和网络审计员的授权，授权过程要求必须有两人在场，并经双重认可后方可操作，操作过程应保留不可更改的审计日志。

6.6.8 主机系统安全管理

税务信息系统的主机系统安全管理的基本要求如下：
a) 各级税务单位信息安全执行机构负责本级税务信息系统的主机系统安全管理；
b) 制定税务信息系统的主机系统安全管理制度，对主机操作系统和数据库管理系统安全相关事项的管理作出明确规定；
c) 主机系统安全管理由安全员按权限实施，包括按《安全员手册》对操作系统、数据库管理系统进行安全机制配置、安全运行控制、软件升级、漏洞及修补等，并对配置文件定期（至少每月一次）进行离线备份；
d) 对系统漏洞进行持续跟踪，每月至少进行一次漏洞扫描，对发现的漏洞，在应对措施经过充分论证后方可进行修补；漏洞修补前应对可能的风险进行评估和充分准备，如选择恰当时间，并做好数据备份和回退方案；漏洞修补后应进行验证测试，以保证系统的正常运行；
e) 主机系统安全审计由审计员按权限实施，包括按《审计员操作手册》对操作系统和数据库管理系统提供的各类审计机制进行配置，对各类审计信息进行存储、汇集、维护和分析等；
f) 根据厂家提供的软件版本升级和补丁，及时对主机系统软件进行版本升级或补丁更新，并在更新前对重要文件进行备份；
g) 应严格控制对系统管理员、系统安全员和系统审计员的授权，授权过程要求必须有两人在场，并经双重认可后方可操作，操作过程应保留不可更改的审计日志。

6.6.9 用户授权管理

税务信息系统用户授权管理的基本要求如下：
a) 各级税务单位信息安全执行机构负责本级信息系统的用户授权管理；
b) 税务信息系统一般用户与系统用户应进行权限分离，不允许一般用户具有系统用户的任何权限；
c) 作为系统用户的税务信息系统管理员、安全员和审计员应分别由不同的人员担任，仅授予其完成各自任务所需的最小权限，并在其登录系统时进行严格的身份鉴别；
d) 税务信息系统的主机系统管理员、网络系统管理员和应用软件系统管理员可由一人承担；税务信息系统的主机系统安全员、网络系统安全员和应用软件系统安全员可由一人承担；税务信息系统的主机系统审计员、网络系统审计员和应用软件系统审计员可由一人承担；
e) 系统用户权限应与终端进行绑定。

6.6.10 备份与恢复管理

税务信息系统备份与恢复管理的基本要求如下：
a) 各级税务单位信息安全领导机构负责本级信息系统的灾难备份与恢复管理；

b) 按《税务系统网络与信息安全事件应急响应工作指南》中关于灾难恢复预案的要求组织实施；
c) 各级税务单位信息安全执行机构负责本级信息系统的常规备份与恢复管理；
d) 制定备份与恢复操作规程，对备份方式、备份频度、备份介质、保存期和操作要求等作出详细规定；
e) 定期或根据需要临时以整体备份或增量备份的方式，备份重要业务数据（至少每天一次）、系统数据及软件系统（至少每月一次）等；重要业务数据包括账户、交易、结算、转账等，系统数据包括权限设置、网络地址、硬件配置及其它重要系统配置参数，软件系统包括系统软件及应用软件的执行程序及可获取的源代码；
f) 在设备、硬件系统发生故障时，及时进行替换并恢复运行；
g) 在系统运行过程中，按操作规程定期（至少每月一次）进行局部系统备份和全系统备份；在发生局部系统故障或全系统故障时，按操作规程及时进行局部系统恢复或全系统恢复；
h) 发生业务数据丢失、破坏时，应采用恢复技术机制所提供的数据恢复功能，将被丢失或破坏的数据恢复为最后一次备份所保留的状态；
i) 在系统中断运行重启后，根据需要将软件系统及相关数据恢复到中断前最后一次备份所保留的状态；
j) 备份介质应按6.6.3中存储介质管理的相关要求进行保存和管理，并定期（至少半年一次）进行恢复演练，检查和测试备份介质的有效性和恢复过程的可行性。

6.6.11 恶意代码防范管理

税务信息系统恶意代码防范管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的恶意代码防范管理；
b) 根据所配备的恶意代码防范产品的操作管理要求，制定恶意代码防范实施细则，对恶意代码防范的责任人、防范部署、防范配置要求、防范软件的使用、升级等作出明确要求；
c) 通过安全意识教育，提高税务系统内部人员及税务系统用户的恶意代码防范意识；
d) 主机与网络应配置不同的恶意代码防范产品，以达到互补的目的；
e) 对恶意代码防范进行统一管理，及时通告恶意代码防范软件版本升级、恶意代码库数据更新要求；定期或根据需要对网络和主机进行恶意代码检测并保存检测记录；定期对恶意代码防范软件的升级以及恶意代码库数据更新情况进行检查，对新发现的恶意代码及时进行分析，报所属信息安全领导机构和相关职能部门；
f) 防范责任人应根据恶意代码防范部署、配置和通告等要求，及时进行恶意代码防范软件版本升级和恶意代码库数据更新；
g) 系统操作人员在读取移动存储设备上的数据以及通过网络接收文件或邮件之前，应先进行恶意代码检查。

6.6.12 安全事件处置管理

税务信息系统安全事件处置管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的安全事件处置管理；
b) 及时报告所发现的安全事件，任何情况下用户均不应自行对安全事件进行尝试性验证；
c) 对出现的安全事件，按《税务系统网络与信息安全事件分级分类指南》的规定进行分级和分类，按《税务系统网络与信息安全报告制度》的要求进行报告；按《税务

系统网络与信息安全信息通报制度》的要求进行通报，按《税务系统网络与信息安全事件调查处理办法》的要求进行调查处理；

d) 对发生的可能涉及国家秘密的重大信息安全事件，应按照有关规定向公安、安全、保密等部门汇报；

e) 严格控制参与涉及国家秘密的安全事件处理的人员，重要操作要求至少两名工作人员在场并登记备案。

6.6.13 应急响应管理

税务信息系统应急响应管理基本要求如下：

a) 各级税务单位信息安全领导机构负责本级信息系统的应急响应管理；

b) 按《税务系统网络与信息安全事件应急响应工作指南》的要求，组织应急响应工作的实施；

c) 发生应急事件时，根据事件的具体情况，启动执行应急响应预案，按预案规定的处理流程、系统恢复流程、事后教育和培训等开展应急响应工作；

d) 从人力、设备、技术和财力等方面，确保应急响应预案的执行有足够的保障；

e) 至少半年进行一次应急响应预案的演练，提高参演人员的预案执行能力；应至少每年进行一次进行综合应急响应预案的全面演练；

f) 定期或根据信息系统变更情况，对应急响应预案进行修订、完善和重新评估；至少应每年进行一次应急响应预案审查，根据实际情况更新应急预案的内容。

6.7 安全变更管理

税务信息系统安全变更管理的基本要求如下：

a) 各级税务单位信息安全领导机构负责本级信息系统的安全变更管理；

b) 制定税务信息系统安全变更管理办法，对信息系统安全变更的处理流程作出明确规定；

c) 由信息系统安全管理执行机构组织实施安全变更工作，在实施后将变更情况向信息安全领导机构报告；

d) 由安全员根据信息系统安全运行情况，提出安全变更需求，经所属信息系统安全管理执行机构报所属信息安全领导机构批准；

e) 在确认信息系统需要进行安全变更以后，由信息安全管理执行机构组织制定安全变更方案，并组织相关人员和专家对方案进行审定；

f) 安全变更的申报、审批和实施等过程应进行文档化管理，记录整个变更过程；

g) 重要系统变更前应制定详细的变更方案、失败回退方案、专项应急预案；

h) 安全变更方案应明确变更失败时对原系统进行恢复的方法和过程，必要时对系统恢复过程组织演练。

6.8 密码管理基本要求

税务信息系统的税务密码管理的基本要求如下：

a) 各级税务单位信息安全执行机构负责本级信息系统的密码管理；

b) 按国家密码管理部门对密码技术和产品的管理要求进行管理和使用；

c) 凡税务总局有统一规定的，应按税务总局的统一规定进行密码技术和产品的管理；

d) 根据国家密码管理部门的有关规定和税务总局的相关要求，制定税务信息系统的密码管理制度；

e) 对税务信息系统配置的密码技术和产品，包括公钥基础设施（PKI）、密钥管理基础设施（KMI）、授权管理基础设施（PMI）和其它密码产品，应按制度要求进行严格管理。

6.9 税务信息系统安全集中管控基本要求

6.9.1 安全策略集中管理

对税务信息系统制定统一的总体安全策略，对以下安全策略进行统一管理：

a) 访问控制策略的统一管理；
b) 应急响应策略的统一管理；
c) 灾难恢复策略的统一管理等。

6.9.2 安全制度集中管理

对税务信息系统安全管理制度进行集中管理，包括：

a) 机房入 / 出管理制度；
b) 安全运行环境管理制度；
c) 一般用户操作管理制度；
d) 系统用户操作管理制度等。

6.9.3 安全机制集中控制

对分散在税务信息系统各组成部分，需要进行集中控制和管理的安全机制，应进行统一、集中控制和管理，包括：

a) 用户身份鉴别机制的统一管理；
b) 访问控制机制的统一管理；
c) 安全审计机制的集中控制；
d) 入侵防范机制的集中控制；
e) 恶意代码防范的集中管理；
f) 备份与恢复机制的集中管理；
g) 密码机制的集中管控等。

6.9.4 安全数据集中管理

对由分散在税务信息系统各组成部分的安全机制获取的安全相关信息，需要进行汇集和管理的，进行集中汇集和管理，包括：

a) 安全审计数据的汇集与管理；
b) 入侵防范机制监测数据的汇集与管理；
c) 恶意代码防范相关数据信息的集中管理；
d) 备份与恢复机制备份数据的集中管理。

6.9.5 安全事件集中管理

对税务信息系统运行过程中发生的各类需要进行集中管理的安全相关事件进行集中管理，包括：

a) 设备状态变化事件的集中管理；
b) 补丁升级事件的集中管理；
c) 安全审计事件的集中管理；
d) 入侵事件的集中管理；
e) 恶意代码事件的集中管理；
f) 备份与恢复事件的集中管理；
g) 安全变更事件的集中管理；
h) 应急事件的集中管理等。

6.9.6 用户授权统一管理

对税务信息系统中需要按统一权限进行管理的用户进行统一授权管理，包括：

a) 按统一的访问控制策略，对分散在税务信息系统各组成部分的一般用户进行统一授权；

b) 按统一的授权管理策略，对税务信息系统各组成部分的管理员、安全员和审计员统一进行授权管理。

6.9.7 密码集中管理

对税务信息系统使用的密码技术和产品进行集中管理，包括：

a) 设置密码集中管理机制，对税务信息系统使用的密码技术进行集中管理；

b) 对PKI进行集中管理：设置CA中心，统一管理CA的相关功能,统一进行证书管理和发放；

c) 对PMI进行集中管理：设置基于PMI的集中授权管理机制，按确定的访问控制策略，对由安全策略覆盖的主、客体进行标记和权限管理；

d) 对KMI进行集中管理：按统一的密码支持机制，进行集中统一的密钥管理；

e) 对其他需要进行集中管理的密码技术和产品进行集中管理。

附录 A

（资料性附录）

相应安全要素的安全基本要求参考表

表 A.1 给出了各安全等级对相应安全功能技术要素的安全技术基本要求。

表 A.1　各安全等级对相应安全功能技术要素的安全技术基本要求参考表

安全功能技术要素	各安全等级安全技术基本要求			
	第一级	第二级	第三级	第四级
1　物理安全技术基本要求	*	*+	*++	*+++
1.1　机房位置选择		*	*+	*+
1.2　机房物理访问控制	*	*+	*++	*+++
1.3　机房防雷击	*	*+	*++	*++
1.4　机房防火	*	*+	*++	*++
1.5　机房防水和防潮	*	*+	*++	*++
1.6　机房防静电		*	*+	*++
1.7　机房温湿度控制	*	*+	*++	*++
1.8　机房供配电	*	*+	*++	*++
1.9　机房电磁防护		*	*+	*++
1.10 设备安全防护	*	*+	*++	*++
1.11 存储介质安全防护	*	*+	*++	*++
2　网络安全技术基本要求	*	*+	*++	*+++
2.1　网络结构安全	*	*+	*++	*+++
2.2　网络访问控制	*	*+	*++	*+++
2.3　网络安全审计		*	*+	*+
2.4　边界完整性保护		*	*+	*+
2.5　网络入侵防范		*	*+	*++
2.6　网络恶意代码防范			*	*
2.7　网络设备登录控制	*	*+	*++	*++
2.8　网络备份与恢复		*	*+	*++
3　主机安全技术基本要求	*	*+	*++	*+++
3.1　用户身份鉴别	*	*+	*++	*+++
3.2　自主访问控制	*	*+	*++	*+++
3.3　标记与强制访问控制			*	*+
3.4　安全审计		*	*+	*+
3.5　入侵防范	*	*+	*++	*++
3.6　恶意代码防范	*	*+	*++	*++
3.7　资源控制		*	*+	*+
3.8　可信路径				*
3.9　可执行程序保护	*	*+	*++	*+++
3.10 备份与恢复				
4　税务应用软件系统安全技术基本要求	*	*	*++	*+++
4.1　用户身份鉴别	*	*+	*++	*+++
4.2　自主访问控制	*	*+	*++	*+++
4.3　标记与强制访问控制			*	*+
4.4　安全审计		*	*+	*+
4.5　检错和容错	*	*	*+	*++
4.6　资源控制		*		*
4.7　可信路径			*+	*+
5　数据保护安全技术基本要求	*	*	*++	*+++
5.1　数据完整性保护	*	*+	*++	*+++
5.2　数据保密性保护		*	*+	*+
5.3　数据交换抗抵赖			*	*+
5.4　数据备份与恢复	*	*+	*++	*+++
6　密码技术基本要求			*	*+
7　安全集中管控技术基本要求			*	*

7.1　安全机制集中控制 7.2　安全数据汇集与管理			* *	* *
注：有“*”号表示有相应安全功能要素的安全技术要求，增加“+”号表示比前一级的要求有增强。				

表 A.2 给出了相应安全管理要素的安全管理基本要求。

表 A.2　相应安全管理要素的安全管理基本要求参考表

安全管理要素	安全管理基本要求
6.1　安全管理机构基本要求	*
6.1.1　安全管理机构设置	*
6.1.2　安全管理机构人员配备及职责	*
6.1.3　安全授权和审批	*
6.1.4　安全管理沟通和合作	*
6.1.5　安全审核和检查	*
6.2　安全管理制度基本要求	*
6.2.1　安全管理制度的内容	*
6.2.2　安全管理制度的制定与发布	*
6.2.3　安全管理制度的评审与修订	*
6.3　人员安全管理基本要求	*
6.3.1　人员岗位管理	*
6.3.2　人员培训与考核管理	*
6.3.3　人员安全意识教育管理	*
6.3.4　外部人员访问管理	*
6.4　税务信息系统安全等级保护管理基本要求	*
6.4.1　定级和备案管理	*
6.4.2　等级测评管理	*
6.4.3　整改和报备管理	*
6.5　税务信息系统安全开发管理基本要求	*
6.5.1　安全设计管理	*
6.5.2　安全产品采购使用管理	*
6.5.3　自行软件开发安全管理	*
6.5.4　外包软件开发安全管理	*
6.5.5　安全工程实施管理	*
6.5.6　安全测试验收管理	*
6.5.7　安全系统交付管理	*
6.5.8　安全服务选择管理	*
6.6　税务信息系统安全运维管理基本要求	*
6.6.1　运行环境管理	*
6.6.2　资产管理	*
6.6.3　存储介质管理	*
6.6.4　设备管理	*
6.6.5　安全审计管理	*
6.6.6　入侵防范管理	*
6.6.7　网络安全管理	*
6.6.8　主机系统安全管理	*
6.6.9　用户授权管理	*
6.6.10 安全变更管理	*
6.6.11 备份与恢复管理	*
6.6.12 恶意代码防范管理	*
6.6.13 安全事件处置管理	*
6.6.14 应急响应管理	*
6.7　密码管理基本要求	*
6.8　税务信息系统安全集中管控基本要求	*
注：有“*”号表示具有相应安全管理要素的安全管理要求。	

6.8.1　安全策略集中管理	*
6.8.2　安全制度集中管理	*
6.8.3　安全机制集中控制	*
6.8.4　安全数据集中管理	*
6.8.5　安全事件集中管理	*
6.8.6　用户授权统一管理	*
6.8.7　密码集中管理	*
注：有“*”表示具有相应安全管理要素的安全管理要求。	