信息安全管理条例

Jan Rautiainen

4/1/2020

文件版本控制

创建人	类型	版本
Jan Rautiainen	内部文件	1.0

文件历史

版本	修改人	日期	修改内容
1.0	Jan Rautiainen	2/4/2020	创建初版

检核历史

版本	检核人	日期	结论
1.0	Steve Collins	3/4/2020	审核通过

审批历史

版本	审批人	日期	审批通过？ (是/否)
1.0	Steve Collins	3/4/2020	是

目录

说明

Take5 员工在区域上的连续性（“T5P”）运营高度依赖于信息资源的管理方式。信息安全管理的策略制定时使用的原则是：

- 支持信息处理的信息资源是重要资产（“信息资产”），必须对其进行适当保护，以防意外或故意泄露。
- 信息资产的机密性、完整性和可用性对于确保法律合规性、保持竞争优以及和 T5P 的形象至关重要。
- 用于支持业务流程的薪资安全管理，会为 T5P 带来收益。
- 所有使用信息资产的人员都有责任保护这些资产，并将不当使用可能造成的风险降至最低。

在整个文件中，“必须”、“应”和“应当”谨慎使用。“必须”和“应”是强制性的，不可协商；“应当”是 T5P 的目标。“数据”、“信息”和“信息资产”在文件中可以互换使用。

信息安全策略和标准

信息安全策略和标准由不同的文档组成：

- 政策

  政策是基于 T5P 要求的高级声明。它们是技术和流程的独立声明，它为 T5P 设定了一般原则、目标和目的，而不仅仅是简单的关于如何实现目标和目的的声明。

- 标准

  标准是安全策略中的下一个层次，业务需求的详细程度是不断提高的。

  标准仍然独立于平台。它们针对的是具体主题领域的政策执行。标准可以进一步细分为两种类型，它们的要求水平各不相同：

  - 需求是必须遵循的活动 – 需求中没有回旋余地。
  - 指导方针不像要求那么严格——应遵循指导方针，除非有令人信服的业务原因不这样做（例如，如果某个司法管辖区内有特定的法律要求禁止实施此类要求，那么就有了令人信服的业务原因不实施此类要求或标准。）

- 程序

  程序是基于流程或者平台需求特定的指导以实现政策或者表内准的执行。一个标准可能需要多个程序-每个平台一个程序来满足该标准。例如，一个处理密码长度的标准要求每个平台（Windows、MacOS、Linux 等）至少有一个单独的过程来实现该标准。

目标

本“信息安全管理条例”文件旨在概述T5P所有的或委托给T5P的任何形式的信息资产的所有用户处理此类信息资产的原则。
这些原则涵盖以下领域：

- 定义用于支持T5P目标的数据和信息资源的机密性、完整性和可用性要求。
- 确保这些数据和安全要求的所有个人都能有效地接触到这些信息。
- 以任何形式（电子或物理）使用、管理和分发这些数据和信息资源的方式始终符合其机密性、完整性和可用性要求。

信息安全的定义

信息安全是保护信息和信息资源不受未经授权的访问、使用、披露、破坏、修改或销毁的关键方法的集合，适用于信息从创建、使用、传输、存储到处置的整个生命周期。

信息安全主要关注数据的机密性、完整性和可用性，而不管数据可能采用何种形式：数字（如数据文件）、材料（如打印纸）或未呈现的信息（如内部事务知识）。包括文字、图片、音频和视频，包括通过邮件、电子邮件、口头交流、电话等方式传输的信息。

T5P要求对所有形式的信息采取适当的控制措施，以确保其机密性、完整性和可用性，并避免违反任何法律、法规、监管或合同义务以及任何安全要求。

- 保密性意味着保护信息不被未经授权的访问或披露
- 完整性意味着保护信息不受未经授权或不适当的修改和破坏
- 可用性是指确保及时可靠地获取和使用数据和信息资源。

T5P还应根据具体情况采取控制措施，确保信息和信息服务的真实性、责任性、不可否认性和可靠性。

- 真实性意味着确保所声称的实体身份的正确性。
- 问责制意味着确保实体对其行动和决定的可追溯性和责任。
- 不可否认意味着防止未来任何实体虚假否认参与。
- 可靠性意味着确保服务的正确性，服务的行为和结果是一致的和可预测的。

范围

本文件用作T5P范围内的信息安全政策，所有与信息资源相关的活动必须遵守这些政策，除非获得本标准批准机构高级管理团队的书面批准。此外，本政策必须公布并传达给所有T5P员工和相关外部方。

目的

这些政策和标准的目的是确保在保护T5P的信息资产时给予应有的谨慎。应有的谨慎是指在T5P及其客户的相同认可的水平上对信息进行经济实用的保护。信息的价值不仅要考虑其开发成本，还要考虑其非货币价值，包括无形价值（如知识产权和竞争价值）和受影响人员的权利（如隐私权）。信息的价值也会受到滥用的影响。良好的信息安全可以通过防止滥用来避免成本。

政策更新评审程序

技术团队中的信息安全官员（“ISO”）负责不时审查和更新本文件，以跟上本政策的任何变化，并在发生变化时请求高级管理团队的批准。

术语和定义

在本套文件中，将使用以下术语：

资产所有者：

资产所有者是指管理层认定的负责维护该资产安全的个人或群体。资产所有者可能在资产的生命周期中发生变化。

- 所有者通常或不一定亲自拥有资产。在大多数情况下，雇用组织、其客户或供应商将是对资产拥有产权的实体。这包括但不限于客户的主数据文档。
- 本文件中使用的术语“资产所有者”是指保留信息的当前实体，该信息被视为一种资产类型。

资产：

资产是对 T5P 及其客户有价值的任何东西。资产有多种类型，包括：

- 信息；
- 软件，如计算机程序；
- 物理，如计算机；
- 服务；
- 人员及其资格、技能和经验；以及
- 无形资产，如声誉和形象。

IT 资产：

IT 资产是与数字信息处理相关的资产。IT 资产的类型包括硬件、软件、数字存储媒体、IT 服务等。

信息资产：

信息资产是资产和 IT 资产的一种。信息资产是对 T5P 或其客户有价值的知识或数据，无论其形式或格式如何。

信息资源：

所有数据、信息以及与这些信息的存储、处理和输出有关的硬件、软件、人员和过程。这包括数据网络、服务器、PC、存储介质、打印机、照片复印机、传真机、支持设备和备份介质。

信息安全策略

1. 归属信息安全组织的成员

T5P的每个成员，包括与T5P签订合同的工作人员和其他可能的第三方实体，负责其控制的信息资源的安全和保护。他/她有义务遵守T5P的信息安全政策、标准、指导方针和程序，保护信息资源不受未经授权的入侵、恶意滥用或无意的损害；并维护这些信息资源的物理和逻辑完整性。

T5P中的以下机构负责管理T5P中的信息安全：

“信息安全官员”（ISO）。这是T5P信息治理结构中的最高权力机构。它代表T5P的管理层，负责批准T5P中有关It规定的政策、指导方针、规则和条例。它还负责就与It相关的计划的资源和预算分配提出建议T5P和IT计划实施的监控和审查。

“高级管理团队”（SMT）。SMT是审查和收集T5P信息安全政策和标准（ISP）意见的机构，SMT由T5P主要高级管理团队的成员组成。

“IT/技术团队”。它包含T5P技术团队的成员。技术团队在维护T5P范围的ISP的同时，还负责满足本ISP的要求。

- ISO负责T5P中所有信息服务和技术的战略发展和协调，还负责所有与安全相关的活动。对T5P范围内的ISP实施情况进行年度审查也是其职责，建议对该ISP进行更改和增强，并建议这些更改由SMT批准。

- SMT负责审查和评估信息安全政策，并将其作为一个整体予以批准。

- IT/技术团队负责提供中央计算设施和技术服务，包括向T5P中的计算机和网络提供服务。IT/技术团队负责实施和管理T5P的中央信息系统。它与不同部门合作，将信息技术纳入行政程序。

“部门”和“信息技术支持单位”。各部门在日常运作中使用T5P的信息。有些部门维持自己的部门资讯科技职能和运作。其工作人员的业务必须满足部门的具体需要。各部门负责人或其代表应确保其信息和信息资源的使用符合T5P范围内的信息安全政策。

“系统所有者”。系统所有者是指负责该特定系统的总体采购、生产、开发、修改、维护和使用的个人或实体。虽然系统所有者对系统的正确操作负有最终责任，但系统所有者可以将部分操作任务委派给IT/技术团队。

2. 信息和 IT 资产清单及所有权

与信息资源相关的重要资产清单必须妥善记录和维护，以备记录和审计之用。
为妥善管理和保护T5P的信息资产，需要建立角色、职责和责任。
T5P获得的、用于工作相关目的或存储T5P或客户信息的所有信息和IT资产均受T5P的控制。只能按照本文件“**4）信息分类和处理**”政策中规定的要求进行处理。

3. 可接受的用途

T5P重视学术和知识自由，鼓励利用T5P的信息资源支持T5P的事务及其教育、服务和研究的使命。必须优先使用T5P官方事务的信息资源。
T5P认可“自带设备”（BYOD）的趋势。无论所有权如何，“信息资源”是指所有信息和通信技术；硬件和软件；数据和相关方法；基础设施和设备。他们有如下特点：

- 由T5P控制或操作；
- 连接到T5P的网络；
- 用于或用于T5P活动；
- 带到T5P的场所。

信息资源包括但不限于：

- 计算机和移动设备-如台式机、笔记本电脑、平板电脑、智能手机、个人数字助理；
- 计算机系统-如T5P的信息系统和应用程序；
- 存储设备——如通用串行总线（“USB”）闪存设备、光盘（“CD”）、数字多功能光盘（“DVD”）、软盘、内置存储器的网络多功能打印机，用于缓存打印输出或存储扫描图像；
- 电信设备——如交换机、路由器、专用交换机（“PBX”）系统和电话、VoIP系统和电话；
- 网络-如通过有线或无线连接的内部网和互联网；

以及其他类似的技术：

- 存储在任何运营商、服务提供商和第三方以及其他此类第三方云存储服务中的信息或数据。

信息资源的使用，包括其处理和存储，必须是合法的，必须符合最高道德标准，不得涉及T5P环境不可接受的活动和材料，包括但不限于恶意或妨害性质的行为，侵犯隐私，侵犯版权和许可证、骚扰、欺凌、黑客攻击、擅自更改任何信息资源的设置、抄袭、冒充/盗用身份或欺骗。

4. 信息分类与处理

T5P必须将其所有信息划分为适当的级别（如受限、机密、内部和公开），以表明需要、优先级和所需的保护程度。
以下分类级别应用于T5P信息资产的分类：

- 受限。本分类适用于受T5P、政府或T5P与第三方（包括政府）之间的任何其他协议严格限制的敏感信息。
- 机密。本分类适用于T5P授权人员使用的敏感信息。
- 内部。本分类适用于部门或T5P内部使用的信息。
- 公开。本分类适用于经授权方在T5P中批准用于公共消费的信息。

T5P的每个成员都有责任在其工作过程中考虑信息的整个生命周期中的安全性。
T5P为某些类型的信息定义了保留期。T5P的每个成员应遵守这些要求。本文件的“16.2）T5P政策和法规”部分列出了T5P政策的一些来源。
各T5P部门应建立与其持有和处理的信息相适应的程序，并确保所有工作人员了解这些程序。

5. 人力资源保障

5.1. 雇用/聘用前

T5P的工作人员和可能的第三方成员必须了解他们的职责，并且必须适合他们在处理或使用信息资产时所考虑的角色。T5P必须实施适当的控制措施，以降低T5P信息资产和资源被盗、欺诈或滥用的风险。

- **角色和职责**。所有T5P的工作人员和可能的第三方用户都有义务遵守T5P及其各自部门定义和记录的安全角色和责任。
- **筛选**。对其角色或职位可能接触敏感信息的候选人来说，就业前筛选是一项强制性要求。
- **承诺**。所有T5P的工作人员必须同意并签署保密承诺，以表明他们完全理解自己在信息安全方面的责任，并同意遵守T5P的信息安全政策。

5.2. 雇佣/聘用期间

T5P的工作人员和可能的第三方用户应了解信息安全威胁和担忧；以及他们的责任和义务；并应配备适当的设备，以支持T5P ISP的正常工作活动，并减少人为错误的风险。

- **管理职责**。T5P的管理层负责确保T5P的所有员工和可能的第三方成员遵守T5P的ISP。
- **信息安全意识、教育和培训**。T5P的所有员工和可能的第三方用户应接受适当的信息安全意识培训，并定期更新与其工作职能相关的T5P ISP。
- **纪律程序**。所有违反安全规定的T5P员工和可能的第三方成员将受到T5P的纪律处分。

5.3. 雇佣/聘用的终止或变更

与第三方员工的雇佣关系或T5P/T5P员工的雇佣关系应以有序的方式退出。

- **资产返还**。在终止雇佣关系和合同关系时，T5P的所有员工和可能的第三方必须以T5P可接受的条件归还其拥有的所有T5P资产。
- **取消访问权**。在责任、雇佣和合同关系终止时，必须取消或取消对信息和/或信息资源的访问权。
- **责任或雇佣的变更**。T5P应管理责任或雇佣的变更以及雇佣或责任的终止。新的职责或雇佣应按照第5.1节的规定进行管理。

6. 物理访问安全

构成 IT 运营的设备、记录和数据是 T5P 的关键资产，必须根据其价值、保密性、存储或访问的信息或数据的重要性以及识别的风险对其进行充分保护。必须对 T5P 的信息资源实施物理访问控制，并应包括以下实施要素：

- 设备控制（进出办公室），如适用；
- 设施（如场所、现场、办公室和房间）安全计划；
- 紧急疏散期间的实际进入控制，包括疏散计划和信息资产保护计划（视情况而定）；
- 物理访问前验证访问授权的程序；
- 维护记录，包括但不限于基础设施变更记录，如添加或删除网段、添加服务器等。；
- 需要了解人员物理访问的程序；
- 为访客（如工作人员、承包商、客户或潜在客户）签到并陪同（如适用）；以及
- 测试和修订物理访问控制（如适用）。

这些适用于所有信息处理设施和场所，包括本地数据中心、综合办公室和为 T5P 提供服务的承包商的场所。

7. 环境安全

环境安全对于 T5P 非常重要，以确保投入可以满足其性能和正常运行时间目标。T5P 的经营场所应受到物理保护，免受火灾、洪水、风、地震、爆炸、内乱、盗窃、抢劫、故意破坏和其他形式的自然和人为风险的损害。

必须对所有业务关键型系统执行以下条件的环境监控，并且强烈建议对所有其他主机和服务器系统进行执行（如果适用）：

- 空调（温度和湿度）；
- 火灾和烟雾探测和控制；
- 电源；
- 不间断电源（“UPS”）装置；
- 漏水；
- 警报和应急系统；以及
- 外部、内部、接地和其他结构保护。

有关部门、负责人人或保管人负责确保这些条件得到遵守。

8. 沟通与运营管理

T5P 必须确保正确和安全处理信息资源的操作程序得到记录，并提供给适当的工作人员和可能的承包商。详细程度应与所处理信息的重要性和相关操作的复杂性相匹配。

T5P 应将工作人员和可能的承包商的职责和责任区分开，以降低未经授权或无意访问、修改或滥用信息资产的风险。隔离级别应与正在处理的信息的机密性和安全性要求相匹配。

9. 变更管理

T5P 必须确保其信息系统、电信设备、软件和其他信息资源的变更不会对 T5P IT 环境的机密性、完整性和可用性造成不利影响，除非获得高级管理团队（SMT）的豁免书面批准。所有变更必须记录、授权并符合 T5P 的操作和安全要求。尤其应记录以下项目：

- 变更请求，包括发起人、批准人、实施人和审核人记录
- 规划和测试变更
- 评估潜在影响，包括安全影响
- 后备程序

T5P 应确保负责变更开发和生产迁移的人员得到适当隔离。当职责不能分离时，应实施补偿控制，例如，主管级员工应定期和/或在变更后审查系统。

T5P 应分配专门的资源来监控变更过程。生产系统的定期系统迁移日志检查应由具有足够技术知识并独立于负责系统的变更团队的人员执行。

10. 网络和平台安全

10.1. 网络隔离

T5P应使用适当的安全措施和适当的设备适当保护所有网络。应妥善维护网络地址、网络配置和相关系统或网络信息，并仅向授权方发布。

T5P应根据网络中承载的信息和服务的用途、分类，将办公网络划分为不同的网络环境：

- **“不可信网络”**。非受信任网络上的设备可供T5P的所有成员访问，或由设备的一般用户或所有者（例如个人平板电脑）完全控制和管理。

  由于这些设备可能被滥用或配置不当，应使用不受信任的网络隔离这些设备。不允许直接访问任何敏感信息或服务器。

- **“管控网络”**。受管控网络上的设备由信息安全部门、IT/技术团队和设备用户管理。在这些设备上实施访问控制，使这些设备仅可供指定用户访问或由一小群指定用户共享（例如工作人员的办公桌）。管理网络应用于T5P部门的日常办公任务和活动。

- **“安全网络”**。关键服务应托管在安全网络中，并且只能由授权员工、适当的可能承包商和第三方成员访问。“受限”和“机密”信息应主要存储在安全网络中，仅在需要时传输到其他网络上的设备进行处理。应实施适当的安全控制，以保护网络中的设备、服务和信息。

T5P应维护多个安全网络，以隔离不同性质或安全要求的服务和应用。

- **“（部门）内部网络”**。部门内部网络是T5P网络中的子网络。它们由各自的T5P部门或受信任的工作人员单独控制和维护。当需要托管和/或处理“受限”、“机密”和“内部”信息时，必须将部门网络分为“不可信网络”、“管理网络”和“安全网络”。这些部门内部网络的安全级别必须符合T5P的信息安全管理政策。

T5P应管理和控制网络，以维护网络安全。工作人员、可能的承包商和第三方成员不得将未经授权的设备连接到网络或以任何方式降低T5P网络的安全级别。网络之间的连接不得损害或降低网络中处理的信息的安全性。

T5P应记录、监测和控制与其网络连接的无线网络。禁止工作人员、可能的承包商和第三方成员连接未经授权的有线/无线网络设备和/或建立点对点或自组织无线网络连接到T5P的网络，并将T5P的网络共享给非受控设备。

应采用适当的认证和加密安全控制，以保护有线/无线网络上与T5P网络连接的数据通信。

10.2. 互联网和外部网络安全

集中安排的互联网网关由IT/技术团队（如适用）管理。T5P部门可根据T5P的现行政策和法规安排和管理自己的互联网网关。

所有网关（包括互联网网关和T5P、T5P合作伙伴和/或T5P远程站点之间的外部网络网关）必须得到IT/技术团队的批准和注册，所有互联网接入应通过注册网关进行。所有网关还必须符合T5P的“网络和平台安全标准”。

所有进出T5P网络和系统的入站和出站流量必须通过注册网关。

“受限”、**“机密”**和**“内部”**数据在通过不受信任的网络传输时必须加密。

在无法满足标准或网络设计满足特殊目的的情况下，it/技术团队应将网络与T5P的其他网络隔离。业主应向it/技术团队注册网络；应实施适当的安全控制，不得将该网络连接到T5P的其他系统。

10.3. 应用、服务和平台安全

信息系统的所有者、控制者或保管者必须确保其信息系统免受威胁，并且必须实施以下措施：

- 防病毒和防火墙系统
- 入侵检测系统（如可行）
- 信息和系统备份系统
- 网络和应用程序日志记录和监控系统
- 应用程序和平台配置管理和强化
- 硬件和软件补丁管理
- 配置管理

11. 访问控制

根据T5P的功能和安全要求对关键、重要信息资产进行访问控制，对于保障T5P内信息资产的机密性、完整性和可用性至关重要。

11.1. 访问控制策略

T5P必须实现以下功能：

- 访问控制，限制对资源的访问，只允许特权实体访问。可以使用以下实现功能之一：
  - 基于角色的访问；
  - 基于用户的访问；
- 检查和记录“安全事件，特别是由系统执行的安全控制活动”；
- 使用和披露T5P信息需要获得同意的授权控制；以及
- 验证实体（数据网络或系统的单个用户或计算过程）的密码控制，该实体声称是该实体。

T5P部门应定期审查授予角色和用户的服务和数据访问权限，以确保相关角色和个人拥有的权限的适当性。

11.2. 密码和屏幕锁定策略

T5P信息系统的所有帐户必须有密码保护，以帮助维护T5P数据的机密性、完整性和可用性，并帮助保护T5P的信息资源。

T5P的每个成员都有责任确保使用强密码，并根据T5P的密码标准维护密码。这是为了通过帮助授权用户合理地避免因密码选择不当而导致的安全和隐私风险，从而降低T5P的总体风险。

T5P还应在所有工作人员的用户台式机和笔记本电脑上实施屏幕锁定政策，但指定或特殊用途的台式机除外，例如网络性能监控控制台。

12. 信息系统获取、开发与维护

T5P必须确保在持有和处理T5P信息资产的任何系统的整个生命周期内，从概念和设计，到创建和维护，再到最终处置，都考虑到信息安全。本政策概述了实现这一目标的基本要求和责任。

12.1. 信息系统的安全要求

任何对IT系统有需求的部门必须在项目启动阶段与IT/技术团队进行讨论。

新系统或现有系统增强的业务需求文档必须包含安全控制的需求。必须通过进行风险评估从一开始就认识到安全漏洞，安全要求必须与功能要求一起制定。

必须在应用程序中设计适当的控制和审计跟踪，以防止错误、丢失和未经授权修改或滥用应用系统中的信息。

应用系统必须实施输入验证，以确保数据输入正确编码和净化（即过滤所有不接受和不支持的输入，拒绝代码、命令和指令的插入和注入，消除缓冲区溢出和除以零，防止路径横向等）。输入验证必须在服务器端和客户端（视情况而定）强制进行。

12.2. 开发和实施中的安全

T5P必须确保在生产环境中实施之前，对IT系统的所有功能和安全特性进行全面测试。

在准备应用软件的开发和测试阶段使用的任何T5P数据都必须受到保护和控制。

安全控制必须应用于生产环境中IT系统的实施。

应用程序必须由不直接参与系统开发的人员根据预定的标准和方法进行长时间的测试。

测试结果必须记录并保留。在应用程序展开之前，测试结果必须由系统所有者接受和批准。

13. 信息安全事件管理

作为任何组织的总体信息安全战略的一个关键部分，有一个结构化的、精心规划的信息安全事件管理方法是必不可少的。

13.1. 责任

IT/技术团队将在T5P内各方的协助下管理所有信息安全事件，包括但不限于高级管理团队、部门主管、研发和运营人员。

ISO应建立并领导信息安全事件响应小组（“ISIRT”），为T5P提供适当的人员，以评估、响应和学习信息安全事件，并提供必要的协调、管理、反馈和沟通。

T5P的所有员工都有责任向IT/技术团队或ISIRT报告任何安全事件。

安全事故包括但不限于：

- 已知的信息安全漏洞，如盗窃；
- 由于安全机制失效而造成的中断或损失，如计算机病毒感染或系统异常行为；以及
- 已知或可疑的安全事件，如系统中断或因黑客攻击（即入侵或DDOS）造成的流量阻塞。

13.2. 信息安全事件报告和响应程序

T5P的工作人员、可能的承包商和第三方用户遇到任何信息被泄露的证据，或发现任何可能暴露、破坏或销毁信息的可疑活动，必须向其直接主管、T5P IT/技术团队或ISIRT报告此类信息。未经ISO授权，个人不得调查“关键”或“重大”安全事件。

必须定义信息安全事件报告程序来处理信息安全事件。该程序将包括以下内容：

- 确定信息安全事件的类型和严重程度；
- 制定行动和联络点的事件报告程序；
- 针对不同类型和严重程度事件的事件响应程序，包括适当的原因分析和识别、控制、与实际或潜在受事件影响者的沟通、向有关当局报告事件，计划和实施适当的纠正措施，以防止再次发生；
- 扣押信息技术设备及相关数据和日志文件，收集和使用审计追踪和类似证据，作为事件管理和调查过程的一部分，并对这些证据进行适当管理，以便在随后的法律或纪律程序中使用；
- 恢复和补救的正式控制，包括所采取行动的适当文件；以及
- 用于对信息资源进行持续监测以发现事件的机制。

13.3. 信息安全事件后审查程序

信息安全事件解决或结束后，需要进行以下审查活动：

•确定从信息安全事件中吸取的教训；以及

•根据从一次或多次信息安全事件中吸取的经验教训，确定信息安全保障实施的改进。

13.4. 信息安全意识培训

T5P部门的负责人和主管应确保定期对其员工进行适当的信息安全意识培训。

培训计划应：

•包括审查T5P的信息安全政策、指导方针、程序和标准，以及为保护敏感信息而制定的部门程序和最佳做法；

•遵守管理特定类别机密信息的法律，如《个人数据（隐私）条例》等。；

•包括诸如密码管理、保护机密信息的最佳实践、事件报告和安全提醒等主题，这些主题涉及个人工作的技术环境中当前的威胁和最近的事件；以及

•让所有T5P员工、可能的承包商和第三方成员了解及时报告信息安全事件。

14. 业务连续性管理

在发生事故或灾难时，需要业务连续性计划（“BCP”）和灾难恢复计划来维持 T5P 的运营。

每个区域办事处都必须制定计划，使其能够以其他方式执行其所需的核心业务，并为其工作环境制定适当的灾后恢复政策和计划。

T5P 的每个信息系统必须有定期的数据备份、紧急情况下持续关键操作的可用设施和灾难恢复计划。虽然 BCP 的开发是一个一般性的业务问题，IT 组件是总体计划的一部分，但拥有 BCP 是提供 T5P 信息安全的“可用性”组件的一个重要因素。

有效的业务连续性管理必须包括以下内容：

- 危机管理小组，是由高级管理小组组成的行政和决策小组，负责在发生事故或灾难时协调业务连续性计划；
- 应急运行中心和运行计划（如适用）；
- 灾难恢复和业务恢复计划；以及
- 定期测试和修订程序。

15. 信息系统内部安全评估

T5P 内部安全团队在 T5P 进行独立的内部安全审计。安全团队的角色和职责由 T5P 内部安全审计章程规定。

T5P 必须确保对 T5P 运营至关重要或包含 T5P 敏感信息的所有信息系统和应用程序及其相关基础设施应作为持续过程进行评估，以提高其运营质量。本政策适用于 T5P 所有部门。

应定期进行信息系统内部评估，以确定 T5P 现有安全框架内的不足和改进机会。这些评估将从人员、流程和技术角度评估 T5P 缓解已识别信息安全风险的能力。这些评估将由了解 T5P 信息安全环境的合格人员执行。

当需要进行内部评估时，应向团队成员提供访问权限。这种访问可能包括但不限于：

- 对任何计算或通信设备的用户级和/或系统级访问；
- 获取可能在各部门或行政司的设备或场所制作、传送或储存的信息（电子、硬拷贝等）；
- 使用计算机系统；
- 访问内部评估期间创建的报告和文件；以及
- 访问交互式监控和记录网络流量。

必须获得有关已识别问题的补救措施和改进机会的管理层响应。