信息安全要求

1. 介绍

供应商和 CWT 已签订协议，根据该协议，供应商同意根据该协议的条款提供服务和/或产品（“**协议**”）。供应商同意其应遵守并应促使代表其行事的第三方遵守本文档中包含的信息安全要求（“**信息安全要求**”）和所需的信息安全措施（“**技术和组织安全措施**”）。信息安全要求以及技术和组织安全措施已纳入协议并成为协议的一部分。

2. 定义

2.1 除非本文另有规定或扩展，否则定义的术语应与协议中规定的含义相同。以下定义的术语应适用于这些信息安全要求。如果本协议中包含的定义与此处的定义存在冲突，则应以本文档中的定义为准，因为它与信息安全要求有关。

除非本协议另有规定，**“关联公司”**系指在本协议签署之日直接或间接控制一方的任何公司或其他法律实体；或（ii）由一方控制；或（iii）由直接或间接控制一方的公司或实体控制。出于这些目的，“控制”是指行使百分之五十（50%）以上表决权或类似所有权的权利；但仅限于这种控制继续存在的情况下。

“**授权员工**”是指需要了解或以其他方式访问机密信息和个人信息以使供应商能够履行其在本协议下的义务的供应商员工。

“**被授权方**”是指供应商的（i）授权员工；（ii）需要知道或以其他方式访问个人信息和机密信息以使供应商能够履行其在本协议下的义务的第三方，并且以书面形式受保密和其他足以保护个人信息和机密信息的义务的约束根据协议和本文件的条款和条件。

“**机密信息**”是指与（a）CWT、其合作伙伴及其附属公司有关的任何商业敏感、专有或其他机密信息；（b）CWT 客户和 CWT 客户雇员、承包商、分包商或供应商；（c）CWT 人员；（d）其独立合作伙伴和合资企业；（e）协议的内容和/或目的，无

论是口头的、书面的或通过任何其他方式可能直接或间接地由供应商或被授权方拥有或与协议。为免生疑问，所有工作产品均构成机密信息。

“**CWT**”（除非协议中另有定义），指协议中概述的 CWT 实体及其关联公司。

“**隔离区**”或“**DMZ**”是位于受信任的内部网络（例如公司专用局域网（LAN））和不受信任的外部网络（例如公共 Internet）之间的网络或子网络。DMZ 有助于防止外部用户直接访问内部系统和其他资源。

“**事件管理流程**”是供应商开发的、记录在案的流程和程序，在发生实际或疑似攻击、入侵、未经授权的访问、丢失或其他涉及机密性、可用性或完整性的破坏时应遵循个人信息和 CWT 的机密信息。

“**掩蔽**”是覆盖屏幕上显示的信息的过程。

“**移动和便携式设备**”是指与本协议相关的、能够轻松携带、移动、运输或传送的移动和/或便携式计算机、设备、媒体和系统。此类设备的示例包括笔记本电脑、平板电脑、USB 硬盘驱动器、USB 记忆棒、个人数字助理（PDA）、移动或数据电话，以及任何其他能够存储机密信息和个人信息的无线、外围或可移动设备.

“**个人信息**”（除非协议中另有定义），是指根据法规（EU）2016/679 和其他适用的全球信息安全、数据保护和隐私法的定义，是指与已识别或可识别的自然人有关的任何信息，这些自然人可以直接或间接识别，特别是通过参考识别号或一个或多个特定于他或她的身体、生理、心理、经济、文化或社会身份的因素。个人信息归 CWT 所有，而非供应商所有。

“**安全网关**”是指具有不同信任级别的两个或多个网络之间的一组控制机制，用于过滤和记录在网络与相关的管理和管理服务器之间通过或试图通过的流量。安全网关的示例包括防火墙、防火墙管理服务器、跳箱、会话边界控制器、代理服务器和入侵防御设备。

“**强认证**”是指使用需要多个认证因素的认证机制和认证方法，包括以下至少两项：（1）知识——用户知道的东西，例如密码或个人识别号码，（2）所有权——一些东西用户拥有，例如令牌、智能卡、移动电话，以及（3）固有-用户是什么，例如指纹。

“**强加密**”是指使用对称加密的最小密钥长度为 256 位和非对称加密的最小密钥长度为 1024 位的加密技术，其强度可合理保证其应保护加密信息免受未经授权的访问，并足以保护机密性和加密信息的隐私，并包含用于管理加密密钥和相关过程的文件化策略，足以保护用作加密算法输入的密钥和密码的机密性和隐私。强加密包括但不限于：SSLv3.0+或 TLSv1.2、点对点隧道协议（PPTP）、AES 256、FIPS 140-2（仅限美国政府）、RSA 1024 位、SHA1/SHA2/SHA3、互联网协议安全（IPSEC）、SFTP、SSH、Vormetric v4 或 WPA2。

“**技术和组织安全措施**”是指根据这些信息安全要求所要求的任何活动访问、管理、传输、处理、存储、保留和销毁信息或数据；根据协议和适用的信息隐私和数据保护法的要求披露和通知受影响的各方；保护信息或数据以确保可用性、完整性、机密性和隐私，或通知个人任何未能保护此类信息或数据的情况。措施包括但不限于欧盟通用数据保护条例（GDPR）、欧盟支付服务指令（EU Payment Service Directive）、加州消费者隐私法案（the California Consumer Privacy Act）、NYS DFS 23 NYCRR 500、美国 Gramm-Leach Bliley Act 法案（GLBA）要求或解释为要求的措施。、美国健康保险流通与责任法案（HIPAA）、欧盟/瑞士数据隐私要求，以及与协议下的信息或数据有关的任何其他国际和美国法律、官方法律解释或案例先例。

“**第三方**”是指供应商的分包商顾问、临时人员、承包商或其他供应商和/或代表供应商行事的代理人，并且确实包括适用的欧盟、美国或其他国际法对第三方的任何定义。

“**供应商**”是指协议中规定的合同实体及其关联公司和第三方。

3. 信息安全组织

供应商应至少：

3.1 确保只有授权方有权访问个人信息和机密信息。

3.2 实施不低于信息安全最佳实践的技术和组织安全措施，以保护机密信息、个人信息和其他非公开信息的完整性、可用性和机密性，并防止未经授权的访问、获取、披露、破坏、更改、个人信息或机密信息的意外丢失、误用或损坏。

3.3 建立、实施和保持与行业最佳实践、政策和组织、运营、管理、物理和技术以及组织安全措施计划相一致，以（1）防止非授权方访问个人信息和机密信息未经协议或这些信息安全要求授权的方式，以及（2）遵守并符合所有适用的法律法规和适用的行业标准。

3.4 向有权访问个人信息和机密信息的授权方提供有关技术和组织安全措施的监督、指导和培训，包括提供与当前威胁情景相一致的实践练习并向接受培训的人员提供反馈的培训。供应商应在授权员工雇用时和授权方访问机密信息和个人信息之前提供技术和组织安全措施培训。应至少每年提供一次进修培训，并在供应商的技术和组织安全措施发生任何重大变化后尽快提供。

3.5 授权方提供专门培训，包括但不限于人力资源或信息技术职能，以及任何技术管理员职能。专业培训至少应包括适用于该角色的信息安全程序、信息安全资源的可接受使用、信息系统的当前威胁、特定系统的安全特性和安全访问程序。

3.6 采取合理措施防止未经授权访问或丢失个人信息和机密信息以及包含此信息的服务、系统、设备或媒体。

3.7 采用风险评估流程和程序定期评估用于向 CWT 提供服务或产品的系统。供应商应尽快补救此类风险，并与识别时已知的威胁对个人信息和机密信息的风险水平相称。运行流程以向供应商安全团队报告风险或可疑事件。

3.8 如果供应商根据本协议在 CWT 设施中执行服务或使用 CWT 拥有、运营或管理的服务、系统、设备或媒体，供应商应促使所有授权方遵守向供应商提供的所有 CWT 政策。请求，适用于此类访问。当被授权方不再需要访问个人信息或机密信息以便供应商向

CWT 提供产品或服务时，供应商应立即以书面形式通知 CWT，包括但不限于当被授权方终止或不再履行职责时协议项下的服务。

3.9 保留访问、传输、维护、存储或处理个人信息和机密信息的授权方和供应商资源的记录。

3.10 在法律允许的范围内，在雇用前对所有授权方进行全面的背景调查。对个人的全面背景调查应至少包括个人以前的工作经历、犯罪记录、信用记录、参考调查以及任何其他行业标准背景调查要求。

3.11 指定一名或多名合格人员负责维护其信息安全计划，并应至少每年向供应商董事会或同等管理机构报告其信息安全计划。供应商应确保其安全人员具有合理和必要的信息安全经验和培训，包括保持对不断变化的威胁和对策的知识。根据要求，供应商应向 CWT 提供所有信息安全相关项目的联系人。

3.12 在向授权方提供对个人信息和机密信息的访问权限之前，要求他们做出不披露或保密的合同承诺。

3.13 确保所有可能根据协议执行工作或可能访问个人信息或机密信息的授权方均遵守这些技术和组织安全措施，这些措施应以不低于这些信息安全要求的书面协议为证.

4. 物理和环境安全

供应商应至少：

4.1 确保供多个用户使用的所有供应商系统和其他资源都位于安全的物理设施中，并且仅限授权个人访问。

4.2 出于审计目的监控和记录，访问包含供多个用户使用的系统和其他资源的物理设施，这些资源与供应商履行其在本协议项下的义务有关。

4.3 要求所有授权方在离开工作区之前遵守清洁桌面政策并锁定工作站屏幕。

4.4 在雇佣终止或合同终止时收集所有公司资产。

4.5 根据以下要求限制和监控对其设施的物理访问：

a. 访客访问被记录下来，保留三（3）个月，包括访客的姓名、他/她所代表的公司以及授权物理访问的员工的姓名。访客必须始终由供应商员工陪同。
b. 基于需要知道的基础，访问仅限于适当的人员。
c. 所有员工必须佩戴公司提供的名牌，所有访客或第三方必须佩戴公司提供的客人/访客证。
d. 供应商人员或第三方终止后，访问将立即撤销，并且所有物理访问机制（例如钥匙、访问卡等）都将被退回或禁用。
e. 数据中心或计算机房被锁定，访问仅限于需要访问以执行其工作职责的人员。
f. 在法律允许的情况下，使用摄像机监控个人对敏感区域的物理访问，并定期审查此类数据。视频片段必须至少保存三（3）个月。
g. 用于存储、处理或传输个人信息和机密信息的设备必须受到物理保护，包括无线接入点、网关、手持设备、网络/通信硬件和电信线路。

4.6 实施控制措施以最大限度地降低风险并防止物理威胁。

4.7 制造商推荐的服务要求，维护所有处理或处理个人信息和机密信息的硬件资产。

4.8 从供应商的内部网络逻辑和物理上限制会议室和其他可公开访问的网络和网络插孔，并且仅限于经过身份验证的用户或默认禁用。

4.9 通过定期检查设备表面以检测篡改或替换，保护通过直接物理交互捕获支付卡数据的任何设备免受篡改和替换；为人员提供培训，使其了解试图篡改或更换设备。

4.10 控制和隔离访问点，例如交付和装载区域以及访问、管理、存储或处理个人信息和机密信息的所有中心的其他点。

4.11 确保供应商数据中心具有加热、冷却、灭火、水检测和热/烟雾检测设备。供应商数据中心和计算机房必须没有可燃材料（例如盒子、纸张等）或存放在金属柜中。

5. 访问控制

供应商应至少：

5.1 采取一切合理措施防止授权方以外的任何人以任何方式或出于未经 CWT 和本协议授权的任何目的访问个人信息和机密信息。

5.2 通过使用物理上独立的服务器或使用未实现服务器物理分离的逻辑访问控制，将 CWT 的信息与供应商的其他客户数据或供应商自己的应用程序和信息分开。

5.3 至少每季度确定并要求适当的所有者审查和批准对用于访问、处理、管理或存储个人信息和机密信息的系统的访问，以消除未经授权的访问；维护和跟踪访问批准。

5.4 授权方终止与供应商的关系后 24 小时内，删除对管理个人信息和机密信息的系统的访问权限；并维持合理的程序,在不再需要或与履行职责相关的三个工作日内取消对此类系统的访问.在闲置 90 个日历日后，必须禁用或删除所有其他用户 ID。

5.5 将系统管理员（也称为 root、特权或超级用户）对旨在供多个用户使用的操作系统的访问权限仅限于在执行工作时需要此类高级访问权限的个人。使用带有个人用户登录凭据和活动日志的签出系统管理员 ID 来管理高安全性访问并减少对数量非常有限的用户的高级访问。要求应用程序、数据库、网络和系统管理员将用户的访问权限限制在他们执行授权功能所必需的命令、数据、系统和其他资源上。系统管理角色和访问列表必须至少每年审查一次。

5.6 执行最小特权规则（即，限制对命令、信息、系统和其他资源的访问，这些资源是根据个人的工作职能执行授权职能所必需的）。

5.7 所有非控制台管理访问、任何远程访问以及对云环境的所有管理访问都需要强身份验证。

5.8 禁止并采用技术和组织安全措施以确保个人信息不能复制、移动或存储个人信息到本地硬盘驱动器或剪切和粘贴或打印个人信息。

5.9 仅在需要时激活远程访问功能的使用，在使用时进行监控，并在使用后立即停用。

5.10 需要强身份验证才能连接到包含个人信息和机密信息的内部供应商资源。

6. 识别和认证

供应商应至少：

6.1 将唯一的用户 ID 分配给各个用户，并将身份验证机制分配给每个单独的帐户。

6.2 使用记录在案的用户 ID 生命周期管理流程，包括但不限于对所有个人信息和机密信息和跨所有环境（例如，生产、测试、开发等）。该过程应包括至少每季度对访问权限和帐户有效性进行审查。

6.3 仅限使用有效用户 ID 和密码的人员访问个人信息和机密信息，并要求唯一的用户 ID 使用以下其中一项：密码或密码、双因素身份验证或生物特征值。

6.4 要求密码复杂性并满足以下密码构造要求：系统密码长度至少为十二（12）个字符，平板电脑和智能手机密码长度至少为四（4）个字符。系统密码必须包含以下三（3）项：大写、小写、数字或特殊字符。密码也不得与与其关联的用户 ID 相同，包含字典单词、连续或重复数字，并且不能是过去 24 个密码之一。要求密码定期过期，不超过九十（90）天。显示时屏蔽所有密码。

6.5 将失败的登录尝试限制为在 24 小时内不超过五（5）次失败的登录尝试，并在达到该限制时将用户帐户锁定为持久状态。随后可以通过需要验证用户身份的手动过程重新激活对用户帐户的访问。

6.6 验证用户的身份并将一次性使用和重置密码设置为每个用户的唯一值。首次使用后系统提示更换。

6.7 使用安全的方法来传递认证凭证（例如密码）和认证机制（例如令牌或智能卡）。

6.8 将服务帐户和代理密码限制为最少 20 个字符，包括大写、小写和数字字符以及特殊符号。至少每年更改一次服务帐户和代理密码，并在任何知道密码的人离职后更改。

6.9 在不活动时间不超过十五（15）分钟后，终止交互式会话，或激活需要身份验证的安全锁定屏幕保护程序。

6.10 使用基于个人信息和机密信息敏感性的身份验证方法。每当存储身份验证凭据时，供应商应使用强加密对其进行保护。

6.11 将系统配置为在最长不活动时间后自动超时，如下所示：服务器（15 分钟）、工作站（15 分钟）、移动设备（4 小时）、动态主机配置协议（7 天）、虚拟专用网络（24 小时）。

7. 信息系统获取、开发和维护

供应商应至少：

7.1 在 CWT 以书面形式为 CWT 品牌产品或服务或为 CWT 开发的产品和软件指定的登录屏幕或页面上显示警告横幅。

7.2 在切实可行的范围内尽快归还所有 CWT 拥有或提供的访问设备，但在任何情况下均不得超过以下日期后的十五（15）天：

a. 本协议到期或终止；
b. CWT 要求归还此类财产的请求；或者
c. 供应商不再需要此类设备的日期。

7.3 采用有效的应用程序管理方法，将技术和组织安全措施纳入软件开发过程，并确保供应商及时实施以行业最佳实践为代表的技术和组织安全措施。

7.4 遵循行业标准的开发程序，包括非生产环境和生产环境之间的访问和代码分离，以及这些环境之间相关的职责分离。

7.5 确保定期评估软件开发的内部信息安全控制并反映行业最佳实践，并及时修订和实施这些控制。

7.6 管理开发过程的安全性并确保实施和遵循安全编码实践，包括适当的加密控制、针对恶意代码的保护以及同行评审过程。

7.7 在发布到生产之前和之后的功能完整的应用程序上进行渗透测试，至少每年一次，并且在对与 OWASP、CERT、SANSTop25 和 PCI-DSS 一致的源代码或配置进行任何重大修改之后。在部署到生产环境之前修复任何可利用的漏洞。

7.8 在非生产环境中使用匿名或混淆数据。切勿在任何非生产环境中使用纯文本生产数据，也切勿出于任何原因在非生产环境中使用个人信息。确保在生产发布之前删除所有测试数据和帐户。

7.9 审查 CWT 批准的开源或免费源代码、软件、应用程序或服务是否存在缺陷、错误、安全问题或不遵守开源或免费源许可条款。供应商应在使用任何开源或免费源代码之前通知 CWT，如果 CWT 批准使用，应向 CWT 提供开源或免费源代码的名称、版本和 URL。供应商声明并保证（a）其在其产品或服务中使用的任何开放或免费源代码均应

根据“许可”开放或免费源代码许可而非限制性、互惠、遗传或 Copyleft 许可获得许可；（b）供应商有权自由修改、改编开放或免费源代码以及将开放或免费源代码组合或包含开放或免费源代码与专有代码，而不受此类修改、改编或组合或专有代码的限制，其中包含开放或免费源代码以及如何获得许可（统称为“衍生作品”）和（c）此类衍生作品不受任何要求许可衍生作品或免费提供的开放或免费源代码许可的约束根据开源或免费源许可条款向第三方提供。

7.10 不共享根据协议创建的任何代码，无论开发阶段如何，在任何共享或非私有环境（例如开放访问代码存储库）中共享，无论密码保护如何。

8. 软件和数据完整性

供应商应至少：

8.1 在防病毒软件可商用的环境中，安装并运行当前的防病毒软件，以扫描并迅速删除或隔离任何系统或设备中的病毒和其他恶意软件。

8.2 将非生产信息和资源与生产信息和资源分开。

8.3 确保团队对所有系统变更使用书面变更控制流程，包括所有生产环境和紧急变更流程的退出程序。包括所有系统变更的测试、文档和批准，并要求管理层批准此类流程中的重大变更。

8.4 如果供应商处理或存储持卡人数据，则建立和维护 PCI 区域。

8.5 对于使用允许修改个人信息和机密信息的数据库的应用程序，启用和维护数据库事务审计日志记录功能，将数据库事务审计日志保留至少一（1）年，其中三个月可立即用于分析。

8.6 在初始实施期间以及在任何重大修改和更新时检查软件以查找和修复安全漏洞。

8.7 对安全组件执行质量保证测试（例如，识别、身份验证和授权功能的测试）以及旨在验证安全架构的任何其他活动。

9. 系统安全

供应商应至少：

9.1 定期创建和更新用于访问、处理、管理或存储个人信息和机密信息的数据流和系统图的最新版本。

9.2 积极监控行业资源（例如：www.cert.org 和相关的软件供应商邮件列表和网站），以便及时通知与供应商系统和其他信息资源有关的所有适用安全警报。

9.3 有效地管理密码密钥，方法是减少对密钥的访问，减少所需的最少数量的保管人，通过使用至少与数据加密密钥一样强的密钥进行加密来存储秘密和私有密码密钥，并与数据加密密钥分开存储在安全的加密设备，在尽可能少的位置。在安装时和至少每两年更改默认密码密钥，并安全地处理旧密钥。

9.4 使用适用的行业标准安全漏洞扫描软件扫描面向外部和内部的系统和其他信息资源，包括但不限于网络、服务器、应用程序和数据库，以发现安全漏洞，确保此类系统和其他资源正确在基于合理和普遍接受的 IT 政策和标准的风险分析产生的时间范围内，至少每季度和在发布应用程序和重大更改和升级之前，加强和识别任何未经授权的无线网络。

9.5 确保所有供应商的系统和其他资源都得到强化，包括但不限于删除或禁用未使用的网络和其他服务和产品（例如：finger、rlogin、ftp 和简单的传输控制协议/互联网协议（TCP/IP）服务和产品）并安装系统防火墙、传输控制协议（TCP）包装器或类似技术。

9.6 在主动操作模式下部署一个或多个入侵检测系统（IDS）、入侵防御系统（IPS）或入侵检测和防御系统（IDP），以监控所有进出系统的流量和其他资源此类技术在商业上可用并在可行的范围内的环境。

9.7 维护与行业最佳实践相一致的漏洞评估结果的风险评级流程，以修复任何系统或其他资源中的安全漏洞，包括但不限于通过行业出版物、漏洞扫描、病毒扫描和安全日志审查发现的漏洞，并针对此类漏洞可能或正在被利用的可能性及时应用适当的安全补丁。关键漏洞评估结果和补丁必须在可用后立即修复，并且在发布后不得超过 7 天。高漏洞评估结果和补丁必须在发布后 30 天内修复。中等漏洞评估结果和补丁必须在 90 个日历日内修复。低漏洞评估结果和补丁必须在 120 个日历日内修复。

9.8 至少每年在内部和外部进行网络和分段渗透测试，并在任何重要的基础设施或应用程序升级或修改之后进行。

9.9 删除或禁用在供应商系统上发现的未经授权的软件，并采用行业标准的恶意软件控制措施，包括在可能用于访问个人信息和 CWT 的所有服务、系统和设备上安装、定期更新和常规使用反恶意软件产品机密信息。在可行的情况下使用可靠且行业最佳实践的防病毒软件，并确保此类病毒定义保持更新。

9.10 在可用于访问个人信息和 CWT 机密信息的所有服务、系统和设备上维护最新软件，包括适当维护操作系统和成功安装合理最新的安全补丁。

9.11 将配置主机操作系统的安全管理职责分配给特定的个人。

9.12 更改所有默认帐户名称和/或默认密码。

10. 监控

供应商应至少：

10.1 的日志数据从创建日志数据之日起至少保留 12 个月，并在合理的时间范围内并应要求将日志和此类数据提供给 CWT，除非协议中另有规定。日志应设计用于检测和响应事件，包括但不限于：

a. 所有个人用户访问个人信息和机密信息
b. 具有管理权限或 root 权限的人员执行的所有操作
c. 所有用户访问审计跟踪
d. 无效的逻辑访问尝试
e. 识别和认证机制的使用和变更

10.2 记录供应商第三方对包含任何个人信息和机密信息的系统的主要系统活动，并制定正式的第三方保证计划，以确保供应商的第三方或分包商拥有适当的安全控制和认证如果 CWT 完成，则进行云安全评估数据驻留在云环境中。

10.3 将安全日志的访问权限限制为授权个人，并保护安全日志免遭未经授权的修改。

10.4 实施变更检测机制（例如：文件完整性监控）以提醒人员对关键系统文件、配置文件或内容文件的未经授权的修改；配置软件每周执行关键文件比较。

10.5 检查一次包含个人信息和机密信息的系统上的所有安全和与安全相关的审计日志是否存在异常情况，并及时记录和解决所有记录的安全问题。

10.6 每日查看所有安全事件、存储、处理或传输持卡人数据的系统组件日志、关键系统组件日志以及执行安全功能的服务器和系统组件的日志。

11. 安全网关

供应商应至少：

11.1 需要对安全网关的管理和/或管理访问进行强身份验证，包括但不限于出于查看日志文件的目的进行的任何访问。

11.2 拥有并使用记录在案的控制、政策、流程和程序，以确保未经授权的用户没有对安全网关的管理和/或管理访问权限，并且管理安全网关的用户授权级别是适当的。

11.3 对电子邮件安全进行强有力的控制，例如配置 DKIM 和 SPF 身份验证协议，以帮助验证来自受信任和经过验证的来源的电子邮件。在接收电子邮件服务器上实施 DMARC。

11.4 至少每六（6）个月一次，通过选择安全网关样本并验证每个默认规则集和配置参数集确保以下几点来确保安全网关配置得到强化：

a. Internet 协议（IP）源路由已禁用，
b. 环回地址被禁止进入内网，
c. 实施了反欺骗过滤器，
d. 不允许广播数据包进入网络，
e. Internet 控制消息协议（ICMP）重定向被禁用，
f. 所有规则集都以“DENY ALL”语句结尾，并且
g. 每个规则都可以追溯到特定的业务请求。

11.5 确保使用监控工具来验证安全网关的所有方面（例如硬件、固件和软件）是否持续运行。

确保所有安全网关都已配置和实施，以便所有非操作安全网关应拒绝所有访问。

11.6 来自不受信任的外部网络的入站数据包必须在隔离区（DMZ）内终止，并且不得允许直接流向受信任的内部网络。流向受信任内部网络的所有入站数据包必须仅源自 DMZ。DMZ 必须通过使用安全网关与不受信任的外部网络分开，并且必须通过使用以下任一方法与受信任的内部网络分开：

a. 另一个安全网关，或
b. 用于将 DMZ 与不受信任的外部网络分开的同一个安全网关，在这种情况下，安全网关必须确保从不受信任的外部网络接收到的数据包被立即删除，或者如果没有被

删除，则仅路由到 DMZ 而不进行其他处理除了可能将数据包写入日志之外，还会执行此类入站数据包。

以下内容只能位于受信任的内部网络中：

a. 未使用强加密存储的任何个人信息和 CWT 机密信息，
b. 正式备案信息副本，
c. 数据库服务器，
d. 所有导出的日志，以及
e. 用于开发、测试、沙箱、生产的所有环境以及任何其他此类环境；和所有源代码版本。

11.7 使用强加密保护的身份验证凭据不得位于 DMZ 内。

12. 网络安全

供应商应至少：

12.1 根据 CWT 的要求，向 CWT 提供逻辑网络图，记录系统和与其他资源的连接，包括路由器、交换机、防火墙、IDS 系统、网络拓扑、外部连接点、网关、无线网络和任何其他应支持 CWT 的设备。

12.2 维护批准、测试和记录所有网络连接以及防火墙和路由器配置更改的正式流程。配置防火墙以拒绝和记录可疑数据包，并限制为仅允许适当和授权的流量，拒绝所有其他流量通过防火墙。每六个月审查一次防火墙规则。

12.3 在每个 Internet 连接处以及任何 DMZ 和内部网络区域之间安装防火墙。任何存储个人信息的系统都必须位于内部网络区域，与 DMZ 和其他不受信任的网络隔离。

12.4 在外围和内部监控防火墙，以根据需要控制和保护进出边界或边界的网络流量。

12.5 安装威胁检测技术，例如网络检测和响应（NDR）、端点检测和响应（EDR）以及扩展检测和响应（XDR），它们提供了一个全面的解决方案来检测和响应各种网络攻击或勒索软件攻击。

12.6 保持书面流程和控制措施到位，以检测和处理未经授权的访问个人信息和 CWT 机密信息的尝试。

12.7 在向 CWT 提供基于 Internet 的服务和产品时，通过实施网络 DMZ 来保护个人信息和机密信息。为 CWT 提供服务的 Web 服务器应驻留在 DMZ 中。任何存储个人信息和机密信息的系统或信息资源（例如应用程序和数据库服务器）都应位于受信任的内部网络中。供应商应将 DMZ 用于 Internet 服务和产品。

12.8 限制来自应用程序处理、存储或传输个人信息和机密信息的未经授权的出站流量到 DMZ 和 Internet 内的 IP 地址。

12.9 当使用基于射频（RF）的无线网络技术为 CWT 执行或支持服务和产品时，供应商应确保通过使用足以保护个人信息机密性的适当加密技术来保护传输的所有个人信息和机密信息和机密信息；但是，前提是在任何情况下，此类加密都应使用不少于 256 位对称加密和 2048 位非对称加密的密钥长度。定期扫描、识别和禁用未经授权的无线接入点。

12.10 云安全–当 CWT 的数据驻留在云上，或供应商使用第三方云环境，包括但不限于基础设施即服务（IaaS）、软件即服务（Saas）和平台即服务（PaaS），供应商必须实施或评估云安全态势管理，以发现并自动修复公共云中的威胁、错误配置、误用和违规行为。

13. 连接要求

13.1 如果供应商已经或将被提供与本协议相关的个人信息和 CWT 机密信息资源的连接，那么除上述内容外，如果供应商已经或被提供与 CWT 环境的连接，供应商应在最低限度：

a. 仅使用双方同意的设施和连接方法将 CWT 的环境与供应商的资源互连。
b. 未经 CWT 事先书面同意，不得建立与 CWT 环境的互连。
c. 在正常工作时间内向 CWT 提供对任何适用供应商设施的访问权，以维护和支持 CW 根据协议提供的任何设备（例如路由器），以连接到个人信息和机密信息资源。
d. 使用 CWT 根据本协议提供的任何设备连接到 CWT 的环境，仅用于提供本协议明确授权的服务和产品或功能。
e. 如果商定的连接方法要求供应商实施安全网关，请维护使用该安全网关的所有会话的日志。这些会话日志必须包含足够详细的信息，以识别最终用户或应用程序、源 IP 地址、目标 IP 地址、使用的端口/服务协议和访问持续时间。这些会话日志必须在会话创建后至少保留六（6）个月。
f. 允许 CWT 收集与访问有关的信息，包括供应商对 CWT 环境的访问。CWT 可能会收集、保留和分析这些信息，以识别潜在的安全风险，恕不另行通知。此信息可能包括来自跟踪文件、统计数据、网络地址以及访问或传输的实际数据或屏幕。
g. 如果 供应商认为存在违规或未经授权的访问，或者如果 CWT 自行决定认为存在违反安全性或未经授权访问或滥用 CWT 数据设施的情况，或根据 CWT 的指示，立即暂停或终止与 CWT 环境的任何互连或任何 CWT 信息、系统或其他资源。

14. 移动和便携式设备

供应商应至少：

14.1 除非使用强加密完全加密，否则不要在移动和便携式设备上存储个人信息和机密信息。

14.2 网络感知移动和便携式设备传输、使用或远程访问的个人信息和机密信息。
a. 当使用非笔记本电脑的网络感知移动和便携式设备访问和/或存储个人信息和机密信息时，此类设备必须能够在通过网络接收到经过适当验证的个人信息和机密信息后删除所有存储的个人信息和机密信息副本。命令。（注意：这种能力通常被称为“远程擦除”能力。）

b. 制定成文的政策、程序和标准，以确保应实际控制非笔记本电脑且存储个人信息和机密信息的网络感知移动和便携式设备的授权方立即启动删除所有设备丢失或被盗时的个人信息和机密信息。
c. 制定书面政策、程序和标准，以确保非笔记本电脑和网络感知的移动和便携式设备在连续登录尝试失败后自动删除所有存储的个人信息和机密信息副本。

14.3 制定书面政策、程序和标准，确保用于访问和/或存储个人信息和机密信息的任何移动和便携式设备：

a. 由授权方实际拥有；
b. 当授权方不实际拥有时，物理上是安全的；或者
c. 在授权方没有实际拥有、没有物理保护或 10 次访问尝试不成功后，及时、安全地删除他们的数据存储。

14.4 在允许访问存储在移动和便携式设备上或通过使用移动和便携式设备存储的个人信息和机密信息之前，供应商应拥有并使用一个流程来确保：

a. 用户是被授权进行此类访问的授权方；和
b. 用户的身份已通过身份验证。

14.5 实施一项政策，禁止使用非供应商或 CWT 管理和/或管理的任何移动和便携式设备访问和/或存储个人信息和机密信息。

14.6 至少每年审查一次对所有供应商管理或管理的移动和便携式设备的使用和控制，以确保移动和便携式设备能够满足适用的技术和组织安全措施。

15. 运输安全

供应商应至少：

15.1 使用强加密在 CWT 控制或供应商控制的网络之外传输个人信息和机密信息，或者在任何不受信任的网络上传输个人信息和机密信息时。

15.2 对于包含纸质格式、缩微胶片或电子媒体的个人信息和机密信息以进行物理传输的记录，请通过安全的快递或其他可以跟踪、安全包装并符合制造商规范的交付方式进行运输。任何个人信息和机密信息都必须在上锁的容器中运输。

16. 静态安全

供应商应至少：

16.1 在存储时使用强加密保护个人信息和机密信息。

16.2 除非存储设备（例如备份磁带、笔记本电脑、记忆棒、计算机磁盘等）受到强加密保护，否则不得在供应商的网络环境（或 CWT 自己的安全计算机网络）之外以电子方式存储个人信息或机密信息。

16.3 不得将个人信息或机密信息存储在可移动媒体（例如 USB 闪存驱动器、拇指驱动器、记忆棒、磁带、CD 或外部硬盘驱动器）上，除非：出于备份、业务连续性、灾难恢复和允许的数据交换目的，以及根据供应商和 CWT 之间的合同要求。如果根据本小节所述的例外情况使用可移动媒体存储个人信息或机密信息，则必须使用强加密保护信息。对于可移动媒体和存储设备，应禁用自动运行。

16.4 在仅限授权人员访问的区域以纸质格式或缩微胶片适当存储和保护包含个人信息或机密信息的记录。

16.5 除非 CWT 另有书面指示，否则在为、通过或代表 CWT 或以 CWT 品牌收集、生成或创建纸质形式和备份媒体的个人信息或机密信息时，确保此类信息为个人信息或机密信息并且在可行的情况下，将 CWT 的此类信息标记为“机密”。供应商承认，个人信息和机密信息属于并将继续归 CWT 所有，无论是否贴上标签。

17. 退货、保留、销毁和处置

供应商应至少：

17.1 CWT 提出请求或协议终止后，在 CWT 提出此类请求或协议终止后三十（30）个日历日内向 CWT 提供任何个人信息和机密信息的副本，而 CWT 不收取额外费用。供应商应在九十日历日（90）内退回或根据 CWT 的选择销毁所有 CWT 的机密信息和个人信息，包括协议中规定的电子、硬质和安全备份副本（a）协议到期或终止，（b）CWT 要求返还个人信息和机密信息，或（c）供应商不再需要个人信息和机密信息来执行服务的日期后几天和协议下的产品。

17.2 如果 CWT 批准将销毁作为返还个人信息和机密信息的替代方案，则由供应商的官员以书面形式证明销毁使个人信息和机密信息不可检索和不可恢复。供应商应在存储个人信息和机密信息的所有位置和所有系统中彻底销毁所有个人信息和机密信息副本，包括但不限于先前批准的授权方。此类信息应按照完全销毁的行业标准程序进行销毁，例如 DOD 5220.22M 或 NIST 特别出版物 800-88，或使用制造商推荐的受影响系统消磁产品。在此类销毁之前，供应商应维护所有适用的技术和组织安全措施，以保护个人信息和机密信息的安全、隐私和机密性。

17.3 以确保信息无法重建为可用格式的方式处理个人信息和 CWT 机密信息。纸张、幻灯片、缩微胶卷、缩微胶片和照片必须通过交叉切碎或焚烧处理。包含等待销毁的个人信息和 CWT 机密信息的材料必须存储在安全的容器中，并使用安全的第三方进行运输。

18. 事件响应和通知

供应商应至少：

18.1 拥有并使用事件管理流程和相关程序，并为此类事件管理流程和程序配备专业资源。立即且在任何情况下不得超过二十四（24）小时，只要发生任何可疑或确认的攻击、入侵、未经授权的访问、丢失或与 CWT 信息有关的其他事件，请通过 iRespond@mycwt.com 通知 CWT、系统或其他资源。

18.2 通知 CWT 后，定期向 CWT 提供状态更新，包括但不限于为解决此类事件而采取的行动，向 CWT 提供一份书面报告，描述事件、供应商在其响应期间采取的行动以及供应商为防止类似事件发生而采取的未来行动计划。

18.3 在未事先通知 CWT 并直接与 CWT 合作通知适用的地区、国家、州或地方政府官员或信用监控服务机构、受此类违规影响的个人之前，不得报告或公开披露任何此类违反 CWT 信息、系统或其他资源的行为，以及法律要求的任何适用的媒体机构。

18.4 制定流程以迅速识别违反安全控制的行为，包括供应商人员或第三方在这些信息安全要求中规定的行为。已确定的违规者应根据适用法律受到适当的纪律处分。尽管有上述规定，违反者仍应受卖方或其第三方的授权。CWT 不应被视为供应商或其第三方人员的雇主。

19. 业务连续性管理和灾难恢复

供应商应至少：

19.1 制定、运营、管理和修改每个地点的业务连续性计划和每个核心技术的灾难恢复计划，以尽量减少 CWT 对供应商服务或产品的影响。此类计划应包括：特定于业务连续性和灾难恢复功能的指定资源、既定的恢复时间目标和恢复点目标、至少每天备份数据和系统、异地存储数据和系统备份和记录、记录保护和应急计划与协议的要求相称，在场外安全地存储此类记录和计划，并确保供应商可以根据需要获得此类计划。

19.2 根据 CWT 的要求，向 CWT 提供书面的业务连续性计划，以确保供应商能够履行其在协议和本文件下的合同义务，包括任何适用的工作说明或服务水平协议的要求。此类计划应在保护个人信息和机密信息的完整性和机密性的同时进行恢复。

19.3 制定安全备份和恢复个人信息和机密信息的程序，其中至少应包括个人信息和机密信息备份副本的传输、存储和处置程序，并应 CWT 的要求提供此类 CWT 的书面程序。

19.4 确保至少每周创建一次对存储的所有个人信息和机密信息或 CWT 使用的系统的软件和配置的备份。

19.5 业务连续性和灾难恢复计划应至少每年更新一次，或在业务和/或技术环境发生重大变化时根据需要经常更新。

19.6 这些计划还应至少每年一次全面执行，或在业务连续性或灾难恢复计划发生任何重大变化后，由供应商自行承担成本和费用。此类演习应确保受影响技术的正常运行和对此类计划的内部认识。

19.7 及时审查其业务连续性计划以解决其他或新出现的威胁源或场景，并根据要求在合理的时间范围内向 CWT 提供计划和测试的高级摘要。

19.8 确保每周七（7）天、每天 24 小时监控所有存放或处理个人信息和 CWT 机密信息的供应商或供应商签约地点，以防止入侵、火灾、水和其他环境危害。

20. 合规与认证

供应商应至少：

20.1 保留与其因这些信息安全要求和供应商遵守本协议有关的义务的履行情况的完整和准确记录，其格式应允许评估或审计不少于三（3）年或更长时间（视需要而定）根据法院命令或民事或监管程序。尽管有上述规定，供应商只需在继续履行本协议后至少保留一（1）年的安全日志。

20.2 允许 CWT 在不增加 CWT 费用的情况下，在合理的提前通知下，对供应商使用的技术和组织安全措施进行定期安全评估或审计，在此期间 CWT 应向供应商提供书面调查问卷和文件请求。对于所有请求，供应商应立即或经双方同意以书面答复和证据（如适用）作出回应。在 CWT 要求 CWT 进行审计时，供应商应安排在该请求后十（10）个工作日内开始安全审计。CWT 可能需要访问设施、系统、流程或程序来评估供应商的安全控制环境。

20.3 应 CWT 的要求，证明其符合本文件，以及对最新版本的 PCI-DSS、ISO27001/27002、SOC2、Cyber Essentials 或供应商和任何分包商或第三方的类似评估的支持认证代表供应商处理、访问、存储或管理。如果供应商无法证明合规性，则应提供书面报告，详细说明其不合规之处及其补救计划以使其合规。

20.4 如果 CWT 自行决定认为发生了未按照本协议和供应商事件管理流程向 CWT 报告的安全漏洞，则安排在二十四（24）小时内开始审计或评估 CWT 要求进行评估或审计的通知。

20.5 在收到评估结果或审核报告后的三十（30）个日历日内，向CWT提供一份书面报告，概述供应商已实施或拟实施的纠正措施以及每个纠正措施的时间表和当前状态。供应商应每三十（30）个日历日向 CWT 更新此报告，报告截至实施之日的所有纠正措施的状态。供应商应在收到评估或审计报告后九十（90）天内或在替代时间段内实施所有纠正措施，前提是双方在不超过三十（30）内以书面形式共同同意该替代时间段供应商收到评估或审计报告的天数。

20.6 PCIDSS 合规性-在供应商处理支付帐号或任何其他相关支付信息的范围内，供应商目前应遵守支付卡行业（PCI-DSS）的最新版本，以处理处理此信息的全部系统并继续这种合规性。如果任何分包商或第三方代表供应商处理、访问、存储或管理信用卡数据，供应商应从该分包商或第三方获取 PCIAOC，并应 CWT 要求提供。如果供应商在处理 PCI 适用数据的整个系统范围的任何部分不符合或不再符合 PCI-DSS，供应商将立即通知 CWT，立即采取补救措施，不得无故拖延，并提供应要求向 CWT 提供此类补救的定期状态。

21. 标准、最佳实践、法规和法律

如果供应商处理、访问、查看、存储或管理与 CWT 人员、合作伙伴、关联公司、CWT 客户有关的个人信息或机密信息；或 CWT 客户员工、承包商、分包商或供应商；供应商应采用不低于适用的全球、地区、国家、州和地方指南、法规、指令和法律要求的技术和组织安全措施。

22. 修改

CWT 保留通过在 CWT 网站上发布最新版本来不时更新或修改这些信息安全要求的权利。除非供应商在发布后三十（30）天内提供反对此类更新或修改的书面通知，否则供应商将被视为已接受它们。

版本 6.1
日期：04.2024