Mandarin

信息安全要求

1. 简介

供应商同意其和代表其向 CWT 提供服务和产品的第三方将遵守本文所包含的信息安全要求（《**信息安全要求**》），这些要求规定了 CWT 所要求的信息安全措施（《**技术与组织安全措施**》）。

2. 定义

除非本文中另有规定或扩展说明，否则定义术语均与主协议中的含义相同。以下定义术语适用于本《信息安全要求》：

“关联企业”是指某一方、公司或其他法律实体，其：（i）控制或直接控制某一方；或（ii）直接或间接被某一方所控制；或（iii）直接或间接被直接或间接控制某一方的公司或实体控制。基于以上目的，“控制”是指行百分之五十（50%）以上投票权或类似所有权的权利；但持续时间仅限于该控制续存的期间，协议另有定义除外。

“协议”是指 CWT 和供应商签订的合同或其他法律文件，协议主要条款另有定义除外。

“机密信息”是指与（a）CWT 及其关联企业、（b）CWT 客户、（c）CWT 员工、（d）CWT 独立合作伙伴和合资企业或（e）协议的内容和/或目的相关的任何商业敏感、专有或其他机密信息，无论是口头、书面，或任何其他形式；该信息由协议产生或与之相关，因而可能直接或间接由供应商、供应商人员、或供应商的员工、代理商、承包商或分包商所有。为避免产生疑问，所有的工作成果均被视为机密信息。

“CWT”是指协议列出的 CWT 实体及其关联企业，协议另有定义除外。

“隔离区”或**“DMZ”**是指位于可信内网（例如企业专用局域网（LAN））和不可信外网（例如公共互联网）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”是指对机密信息和个人信息的机密性、可用性或完整性造成实际或疑似攻击、入侵、非法访问、丢失或其他破坏时，由供应商开发、文档化的流程和程序。

“屏蔽”是掩盖显示在屏幕上信息的过程。

“移动和便携式设备”是指与协议相关、便于携带、移动、运输或输送的移动和/或便携式计算机、设备、介质和系统。此类设备包括笔记本电脑、平板电脑、USB 硬盘驱动器、USB 记忆棒、掌上电脑（PDA）、移动或数据电话，以及其他任何可以存储机密信息和个人信息的无线或外围设备。

“个人信息”是指根据欧盟条例 Regulation (EU) 2016/679 和其他适用全球信息安全、数据保护与隐私法规定义，与已识别或可识别的自然人相关的任何信息。这些人士是指可被直接或间接识别的自然人，特别是通过参考识别号码，或通过与其物理、生理、心理、经济、文化或社会身份特定相关的一个或多个特征来识别。协议另有定义除外。

“安全网关”是一组控制机制，处于两个或多个具备不同信任等级的网络之间，能够过滤和记录网络以及相关管理服务器之间通过或试图通过的流量。安全网关的具体实例包括防火墙、防火墙管理服务器、hop box、会话边界控制器、代理服务器和入侵防御设备。

“强认证”是指使用比本文要求的密码更严苛的认证机制和方法。强认证机制和方法的具体实例包括数字证书、二元认证和一次性密码。

“强加密”是指使用最低密钥长度为 256 位的对称加密以及 1024 位的非对称加密，其强度足以确保其保护加密信息免受未经授权的访问，并足以保护加密信息的机密和隐私，它还包括一项文档化的政策，用于管理加密密钥和相关流程，足以保护用作加密算法输入的密钥和密码的机密与隐私。强加密包括但不限于：SSL v3.0+/TLS v1.0+、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、互联网安全协议（IPSEC）、SFTP、SSH、Vormetric v4 或 WPA2。

《技术和组织安全措施》是指本《信息安全要求》要求的各项活动，用于访问、管理、传输、处理、存储、保留和销毁信息或数据；披露与通知协议和适用信息隐私与数据保护法要求的受影响方；以及保护信息或数据，以确保其可用性、完整性、机密性和隐私，或通知个人未能保护此类信息或数据安全的情况。具体措施包括但不限于根据以下规定要求或间接要求的措施：在各成员国颁布的欧盟指令 94/46/EC 和 2006/24/EC、美国《格雷姆-里奇-比利雷法案》（GLBA）、美国《健康保险可携性及责任法案》（HIPAA）、欧盟/瑞士数据隐私要求，以及与协议信息或数据相关的任何其他国际和美国法律、正式法律解释或先例。

“第三方”是指各分包商、供应商的各临时员工、承包商，或代表供应商的其他供应商和/或代理商，以及根据适用的欧盟、美国或其他国际法律定义的第三方，协议另有定义除外。

“供应商”是指协议规定的承包实体及其关联企业和第三方。

供应商保证并声明，在适用于协议的服务规定范围内，遵守以下《技术与组织安全措施》：

3. 信息安全组织

供应商：

3.1 应建立、实施并维护与行业实践相一致且合理的政策和一项有组织、可操作、可管理以及符合《技术和组织安全措施》的物理计划，以（1）防止未经协议或《信息安全要求》的授权而访问机密信息和个人信息，以及（2）遵守并满足所有的适用行业标准。供应商还应确保其安全人员在信息安全方面具备合理及必要的经验。

3.2 应根据《技术与组织安全措施》，向其需要访问机密信息和个人信息的员工提供级别相当的监督、指导和培训。供应商还应在招聘时和访问机密信息和个人信息前提供《技术与组织措施》培训。回顾培训应至少每年进行一次，并在供应商的《技术与组织安全措施》出现任何重大改变时尽快提供。

3.3 承担重大安全责任（包括但不限于人力资源或信息技术职责以及任何技术管理工作）的供应商工作人员也应接受与其职责相对应的专业培训。专业培训应包括适用于具体职责的信息安全程序、许可使用的信息安全资源、信息系统当前的威胁、特定系统的安全特性，以及安全访问程序。

3.4 应采取合理措施，以防止机密信息和个人信息以及与包含该信息的服务、系统、设备或介质受到未经授权的访问，或出现丢失。

3.5 应采用风险评估程序来定期评估向 CWT 提供服务或产品的系统。鉴于威胁在识别时已经知晓，供应商还应使用与机密信息和个人信息标注的风险等级相当的措施，尽快修复这些风险。执行某一程序，要求供应商员工向供应商安全团队报告风险或可疑事件。

3.6 供应商按照协议在 CWT 内部设施执行服务、或使用由 CWT 拥有、经营或管理的服务、系统、设备或介质执行服务时，应遵守进行该访问要求的所有适用 CWT 政策。当该访问不再需要时（包括但不限于当某员工、承包商、分包商或供应商的第三方不再按照协议执行服务，或当其不再访问机密信息和个人信息时），还应立即书面通知 CWT。

3.7 应对其访问、传输、维护、存储或处理机密信息和个人信息的资源始终记录。

3.8 应在法律需要和允许的范围内，或根据适用的工作/工单/采购订单的规定，遵守 CWT 的背景调查要求。

4. 物理与环境安全

供应商：

4.1 应确保其供多用户使用的系统和其他资源位于安全的物理设施中，且设置访问权限，仅供授权用户使用。

4.2 应按照审计目的，监控并记录对物理设施的访问，此类设施包含供多用户使用的系统和其他资源，这些使用受供应商履行协议的义务约束。

4.3 应确保其所有员工均在访问机密信息和个人信息前与其签订保密协议。

4.4 应要求其所有员工遵守清理办公桌政策，并在离开工作场所前锁定工作站屏幕。

4.5 应在雇佣关系终止或合同终止时收回所有的公司资产。

4.6 应根据以下要求，限制并监控对其设施的物理访问：

a. 记录访问者的访问，且将日志保存三（3）个月；记录需包括访问者的姓名、他/她代表的公司，以及授权物理访问的员工姓名。
b. 根据须知访问要求，访问仅限于适当人员。
c. 所有员工都必须佩戴公司提供的名牌。
d. 访问权限在合同终止时立即被撤销，所有的物理访问机制（如钥匙、门禁卡等）都应退回或被禁用。
e. 锁定数据中心或机房，仅限需要访问以履行工作职责的人员访问。
f. 使用摄像头监控个人对敏感区域的访问，并定期检查这些数据。视频录像必须至少存储三（3）个月。
g. 用于存储、处理或传输机密信息和个人信息的设备必须进行物理防护，包括无线接入点、网关、手持设备、网络/通信硬件，以及电信线路。

4.7 应实行控制，以尽可能减少风险并预防物理威胁。

4.8 应维护根据第三方服务提供商推荐的服务要求而加工或处理机密信息和个人信息的所有硬件资产。

4.9 应限制会议室和其他可从供应商的网络公共访问的网络接口，仅限已认证身份的用户使用或默认禁用。

4.10 应保护通过直接物理接触获取支付卡数据的设备，通过定期检查设备表面，防止其被篡改或替换；培训员工，使其提防被试图篡改或替换设备。

4.11 应控制并分离访问节点（例如发送和加载区）和来自访问、管理、存储或处理机密信息和个人信息的所有中心的其他节点。

4.12 供应商数据中心必须具备加热、冷却、消防、水检测和热/烟雾检测设备。

5. 访问控制

供应商：

5.1 应采取一切合理措施，防止任何人员以未经 CWT 和协议授权的任何方式或目的访问机密信息和个人信息。供应商应还仅允许其满足以下条件的员工访问机密信息和个人信息：（1）根据协议有合理需求访问机密信息和个人信息以提供服务，且（2）已书面同意保护机密信息和个人信息的完整性、可用性和机密性。

5.2 应保持合理的程序，以便在机密信息和个人信息不再需要或不再与履行供应商员工的职责相关时， 以及在雇佣结束前，终止其对该信息的访问。

5.3 应将 CWT 的信息与其他客户或供应商的自有应用和信息分离，可采用物理上独立的服务器，或者在服务器的物理独立无法实施时，使用逻辑访问控制。

5.4 应识别并要求适当的所有者检查及批准访问用于访问、处理、管理或存储机密信息和个人信息的系统；且应维护及追踪访问批准。

5.5 在员工、承包商、分包商或第三方终止其与供应商的关系 24 小时内，应移除对管理机密信息和个人信息的系统的访问权限；当员工、承包商、分包商或第三方公司内部发生职责变动时，应在三（3）个工作日内移除对此类系统的访问权限。所有的其他用户 ID 必须在闲置 90 天后被禁用或移除。

5.6 应定期检查及批准对管理机密信息和个人信息的系统的访问权限，至少每季度进行一次，以便及时移除未经授权的访问。

5.7 对以系统管理员（也称 root 用户、特权用户或超级用户）身份访问供多用户使用的操作系统进行限制，仅允许为完成工作需要此类高级访问的个人。条件允许时，使用含有个人用户登陆信息和活动日志的检出 ID 来管理高级安全访问，否则就减少有严格用户数量限制的高级访问。

5.8 要求应用、数据库、网络和系统管理员对用户的访问权限进行限制，使其仅可访问执行授权功能必需的命令、数据、系统和其他资源。

5.9 对任何远程访问要求进行强认证。

5.10 禁止及采用《技术和组织安全措施》，以确保访问机密信息和个人信息的供应商员工不得将机密信息和个人信息复制、移动或存储到本地硬盘驱动器，或剪切、粘贴或打印机密信息和个人信息。

5.11 仅在需要时激活远程访问功能的使用；在使用时需进行监控，使用后立即关闭。

5.12 要求至少二元认证方可连接至包含机密信息和个人信息的内部供应商资源。

6. 身份识别与认证

供应商应：

6.1 为个人用户分配唯一的用户 ID，并为单个个人账户分配认证机制。

6.2 针对所有对机密信息和个人信息的访问以及所有环境（例如生产、测试、开发等）中的访问，使用文档化的用户 ID 生命周期管理流程（包括但不限于批准账户建立程序、及时删除账户，以及账户修改，如包括更改权限、访问跨度、功能/角色等）。这些流程应包括对访问特权和账户有效性的检查，至少每季度进行一次。

6.3 强制执行最小特权原则，即根据某人的工作职能执行授权功能时仅能访问必需的命令、信息、系统和其他资源。

6.4 应对机密信息和个人信息的所有访问仅限于使用有效的用户 ID 和密码的人员，并要求唯一的用户 ID 采用以下方法之一进行访问：密码或口令、二元认证或生物特征值。

6.5 要求密码具备复杂性，并满足以下密码结构要求：系统密码长度至少为八（8）位字符，平板电脑和智能手机密码至少四（4）位。系统密码必须包含以下三（3）项：大写字母、小写字母、数字或特殊字符。密码还不能和与其相关的用户 ID 相同、包含字典单词、顺序或重复数字，也不能是过去五个密码之一。要求密码定期失效，周期不超过九十（90）天。显示时屏蔽所有密码。

6.6 24 小时内尝试登陆失败次数不得超过五（5）次，否则用户账户将被持续锁定。可通过手动程序验证用户身份后重新激活对用户账户的访问。

6.7 验证用户身份，并为每个用户设置一次性使用密码，重置为唯一值。第一次使用后系统会提示变化。

6.8 使用安全方法传输认证信息（如密码）和认证机制（如令牌或智能卡）。

6.9 规定服务账户和代理密码至少为 12 位字符，包括大写字母、小写字母、数字字符和特殊符号。至少每年更改一次服务账户和代理密码。

6.10 闲置不超过十五（15）分钟后，终止互动会话或激活需要身份认证解锁的安全锁定屏保。

6.11 使用基于机密信息和个人信息敏感性的认证方法。无论认证信息何时被存储，使用强加密进行保护。

6.12 将系统配置为达到以下闲置期后自动超时：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：

7.1 对 CWT 品牌产品或服务，或为 CWT 开发的产品和软件，按 CWT 书面规定在登陆屏幕或页面时显示警示信息。

7.2 确保所有根据协议开展工作的员工遵循本《技术与组织安全措施》的规定，且由严格程度不低于本《信息安全规定》的书面协议证明其合规性。

7.3 根据实际情况尽快归还 CWT 拥有或提供的所有接入设备，但不得超过以下日期后的十五（15）天：

(a) 协议到期或终止时；
(b) CWT 要求返还此类资产时；或
(c) 供应商不再需要此类设备之时。

7.4 采用将《技术与组织安全措施》纳入软件开发流程的有效应用管理方法，并确保供应商及时实施 CWT 的软件开发周期或信息安全政策、标准和程序中涉及的《技术与组织安全措施》。

7.5 遵守标准开发程序，包括分离非生产和生产环境之间的访问和代码，以及分离其间的相关职责。

7.6 确保对软件开发的内部信息安全控制进行定期访问，确保其反映行业最佳做法，并及时修订和实施此类控制。

7.7 管理开发过程中的安全，确保实施及遵守安全编码规定，包括适当的密码控制、防止恶意代码，以及同行评审流程。

7.8 在投入生产之前及之后至少每年一次，对功能完备的应用进行渗透测试，在根据 OWASP、CERT、SANS Top 25 或 PCI-DSS 标准对源代码或配置进行任何重大修改后也需安排测试。在配置生产环境前修复任何可利用漏洞。

7.9 在非生产环境中使用匿名或混淆数据。在非生产环境中，切勿使用纯文本生产数据，也不要出于任何原因使用机密信息和个人信息。确保所有的测试数据和账户在生产发布前均被删除。

7.10 确保使用开源代码、软件、应用或服务的供应商在检查生成的此类代码，以查明其可能影响 CWT 或 CWT 客户数据完整性、可用性或机密性的各种缺陷、漏洞或安全问题时，进行尽职调查。供应商还应告知 CWT 何处使用开源代码并向 CWT 提供开源代码的名称和版本。

7.11 确保供应商不会在任何情况下分享根据该协议生成的任何代码（无论处在何种发展阶段和任何共享或非私有环境中），例如开放访问代码库（无论是否存在密码保护）。

8. 软件和数据完整性

供应商应：

8.1 安装市场上可买到最新杀毒软件并运行扫描，以便及时从任何系统或设备中删除或隔离病毒和其他恶意软件。

8.2 将生产信息与资源和非生产信息与资源分离。

8.3 确保在所有系统变更时的变更控制流程文档化，包括针对所有生产环境和紧急变化流程的回退程序。在所有的系统变更中都包含测试、记录和批准，对该流程中的重大变更还要求管理层的批准。

8.4 处理或存储持卡人数据时，建立并维护一个 PCI 区。

8.5 对使用了允许修改机密信息和个人信息的数据库的应用，保持数据库事务审计日志功能启用，并将该日志保留至少六（6）个月。

8.6 在软件初始安装以及出现重大修改和更新时进行检查，以便发现并修复其安全漏洞。

8.7 在初始安装以及出现重大修改和更新时，为安全组件进行质量保证测试（例如身份识别、认证和授权功能测试）以及其他用以验证安全架构的活动。

9. 系统安全

供应商应：

9.1 定期创建和更新用来访问、处理、管理或存储机密信息和个人信息的最新版本数据流和系统图。

9.2 积极追踪行业资源（如、www.cert.org 和相关软件供应商邮件列表和网站），以便及时获取与供应商系统有关的所有适用安全警报和其他信息资源。

9.3 使用尽可能少的管理员减少密钥访问从而有效管理加密密钥，使用强度至少与数据加密密钥相当的密钥加密来存储保密和私有加密密钥，并在尽可能少的位置用安全加密设备独立于数据加密密钥存储。安装时更改默认的加密密钥，至少两年更改一次，并安全处置旧密钥。

9.4 至少每季度一次，以及在应用发布前，以及根据合理及普遍接受的 IT 政策与标准、由风险分析引起一定时间范围内的重大更改和任何更新时，扫描面向外部的系统和其他信息资源（包括但不限于网络、服务器和应用），采用适当的行业标准安全漏洞扫描软件来发现安全漏洞。

9.5 至少每季度一次，以及在应用发布前，以及根据合理及普遍接受的 IT 政策与标准、由风险分析引起一定时间范围内的重大更改和任何更新时，扫描内部系统和其他信息资源（包括但不限于网络、服务器、应用和数据库），采用适当的行业标准安全漏洞扫描软件来发现安全漏洞，确保该系统和其他资源被正确强化，并查找出任何未经授权的无线网络。

9.6 根据行业最佳做法和潜在影响保持对漏洞评估结果的风险评级流程。CVSS 分值在 4 分或更高的所有评估结果都必须通过正式方法来处理，以确保风险评估的持续性得到管理。

9.7 确保供应商的所有系统和资源保持被“强化”，包括但不限于删除或禁用未使用的网络、其他服务和产品（例如 finger、远程登陆、ftp 以及简单的传输控制协议/互联网协议（TCP/IP）服务和产品）以及安装系统防火墙、传输控制协议（TCP）包装或类似技术。

9.8 在该技术已进入商用领域的环境下，并在可行的范围内，以主动操作模式部署一个或多个入侵检测系统（IDS）、入侵防御系统（IPS）或入侵检测与防御系统（IDP），该模式监控与协议相关的所有进出系统的流量和其他资源。

9.9 保持风险评级流程来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发布、漏洞扫描、病毒扫描，以及安全日志检查），一旦发现该漏洞有可能或正处于被利用的过程中，

立即采取适当的安全补丁。CVSS 分值为 7.5 分或更高的关键补丁一旦可用，应立即安装，且不得超过补丁发布后一个月。CVSS 分值为 4 分或更高的补丁必须在发布 90 天内安装。

9.10 每年至少开展一次内部和外部的一般渗透测试，在任何重大基础设施或应用升级或修改后也应进行该测试。

9.11 删除或禁用供应商系统中未经授权的软件，并对恶意软件采取行业标准的控制措施，包括在所有可访问机密信息和个人信息的服务、系统和设备上反恶意软件产品的安装、定期更新和常规使用。条件允许时，使用可靠的及行业最佳的防病毒软件，并确保该病毒定义保持更新。

9.12 为可访问机密信息和个人信息的所有服务、系统和设备维护最新软件，包括适当维护操作系统和成功安装合理的最新安全补丁。

9.13 分配安全管理职责，以便为具体人员配置主机操作系统。

9.14 更改所有的默认账户名和/或默认密码。

10. 监控：

供应商应：

10.1 保留机密信息和个人信息的日志数据至少维持 12 个月，并确保该数据根据要求在合理的时间范围内对 CWT 可用，除非协议另有规定。

10.2 为包含任何机密信息和个人信息的系统记录主要系统活动。

10.3 安全日志仅限授权人员访问，防止安全日志受到未经授权的修改。

10.4 采用更改检测机制（例如文件完整性监控）提醒员工注意未经授权修改关键系统文件、配置文件或内容文件的情况；配置软件以便每周进行关键文件比较。

10.5 以至少每周一次的频率对包含机密信息和个人信息的系统进行检查，检查所有的安全和安全相关审计日志是否存在异常，并及时记录和解决日志记录的所有安全问题。

10.6 每天检查所有安全事件，存储、处理或传输持卡人数据的系统组件的日志，关键系统组件的日志，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：

11.1 对安全网关相关的管辖和/或管理访问要求强认证，包括但不限于任何出于检查日志文件目的的访问。

11.2 具备及使用文档化的控制、政策、流程和程序，以确保未经授权的用户无访问安全网关的管辖和/或管理访问权，并且被授权用户具备管理安全网关的适当级别。

11.3 至少每六（6）个月一次，通过选择安全网关样本，以及验证每个默认规则集和配置参数集，确保安全网关配置被强化，确保满足以下条件：

a. 互联网协议（IP）源路由被禁用，
b. 环回地址禁止进入内部网络，
c. 采用反电子欺骗过滤器，
d. 广播数据不允许进入网络，
e. 互联网控制消息协议（ICMP）重定向被禁用，
f. 所有规则集均以“拒绝所有”描述结束，且
g. 每条规则可追溯到一个特定的业务请求。

11.4 确保监控工具被用于验证安全网关的各部分（例如硬件、固件和软件）都连续运行。

11.5 确保所有的安全网关均已配置及实施，使所有的非运作安全网关均拒绝所有访问。

11.6 确保来自不可信外网的入站数据包必须在隔离区（“DMZ”）中终止，且不允许直接流向可信内网。所有流向可信内网的入站数据包只能产生于 DMZ 中。DMZ 必须采用安全网关与不可信外网分离，并通过以下方法之一与可信内网分离：

a. 另一个安全网关；或
b. 用来分离 DMZ 与不可信外网的同一安全网关，这种情况下，安全网关必须确保从不可信外网中接收的数据包或者直接被删除，或者如果未删除，则应确保该入站数据包不经任何其他处理（除了有可能将数据包写入日志外）仅能路由至 DMZ。

以下内容只能存储于可信内网中：

a. 未使用强加密存储的任何机密信息和个人信息，
b. 从不可信外网发起请求而访问的信息的正式记录副本，
c. 从不可信外网发起请求而修改的信息的正式记录副本，
d. 数据库服务器，
e. 所有的导出日志，以及
f. 所有用于开发、测试、沙箱、生产的环境和任何类似环境；以及所有的源代码版本。

11.7 未使用强加密保护的身份认证不能存储于 DMZ 中。

12. 网络安全

供应商应：

12.1 根据 CWT 的要求，向 CWT 提供记录系统以及与其他资源（包括路由器、交换机、防火墙、IDS 系统、网络拓扑结构、外部连接点、网关、无线网络，以及支持 CWT 的任何其他设备）连接情况的逻辑网络图。

12.2 保持正式流程，以便批准、测试和记录所有的网络连接和对防火墙与路由器配置的更改。配置防火墙，以拒绝并记录可疑数据包，只允许适当的授权流量，拒绝所有其他流量通过防火墙。每六个月检查一次防火墙规则。

12.3 在每个互联网连接处，以及 DMZ 和内部网络区之间安装防火墙。任何存储机密信息和个人信息的系统都必须位于内部网络区，与 DMZ 和其他不可信网络隔离。

12.4 必要时，在外围和内部监控防火墙，以控制和保护进出边界的网络流量。

12.5 保持文档化的流程和控制措施，以便检测和处理未经授权尝试访问机密信息和个人信息的行为。

12.6 向 CWT 提供基于互联网的服务和产品时，实施网络 DMZ 来保护机密信息和个人信息。向 CWT 提供服务的 Web 服务器应驻留在 DMZ 中。存储机密信息和个人信息的任何系统或信息资源（例如应用和数据服务器）均应驻留在可信内网中。（互联网服务和产品必须使用 DMZ）。

12.7 限制来自 DMZ 和互联网中处理、存储或传输机密信息和个人信息至 IP 地址的应用的未经授权出站流量。

12.8 使用基于无线联网技术的无线射频（RF）为 CWT 提供或支持服务与产品时，确保传输的所有机密信息和个人信息均采用强加密技术进行保护，足以保护其机密性。定期扫描、识别和禁用未经授权的无线访问节点。

13. 连接要求

供应商应：

13.1 当供应商拥有，或应当获得与协议相关的机密信息和个人信息资源连接时，则：

a. 仅使用双方关于设施和连接方法达成的一致意见对机密信息和个人信息资源与供应商的信息资源进行互联。
b. 未经 CWT 同意，不得建立与机密信息和个人信息的互联。
c. 在正常工作时间内，向任何适用的供应商设施提供 CWT 访问，以便维护及支持由 CWT 根据协议提供的、用于连接机密信息和个人信息资源的各种设备（如路由器）。
d. 使用 CWT 根据协议提供的、用于连接机密信息和个人信息资源的各种设备时，仅限于提供协议明确授权的服务、产品或功能。
e. 如果双方约定的连接方法要求供应商采用安全网关，则使用该网关维护所有会话日志。这些会话日志必须包括足够详细的信息，以便识别最终用户或应用、源 IP 地址、目的 IP 地址、使用的端口/服务以及访问持续时间。这些会话日志必须自会话创建起至少保留六（6）个月。

13.2 当供应商拥有，或应当获得与协议相关的机密信息和个人信息时，除本文规定的其他权利外，CWT 还可：

a. 收集与访问有关的信息，包括供应商对机密信息和个人信息资源的访问。该类信息可被 CWT 收集、保留和分析，以识别潜在的安全隐患，无需另行通知。该类信息可能来自跟踪文件、统计数据、网络地址，以及访问或传输的实际数据或屏幕。
b. 如果 CWT 自认为 CWT 的数据设施或 CWT 的任何信息、系统或其他资源存在违反安全、未经授权的访问或滥用现象，可立即暂停或终止一切与机密信息和个人信息的互联。

14. 移动和便携式设备

供应商应：

14.1 使用强加密保护 CWT 存储在移动和便携式设备上的所有机密信息和个人信息。

14.2 不在移动设备或笔记本电脑上存储机密信息和个人信息，也不在可移动设备上存储机密信息和个人信息（除非使用强加密）。

14.3 使用强加密保护通过网络感知移动和便携式设备传输或远程访问的机密信息和个人信息。

a. 使用笔记本电脑以外的网络感知移动和便携式设备来访问和/或存储机密信息和个人信息时，一旦在网络中收到适当的身份认证指令，该设备必须能够删除存储的所有机密信息和个人信息副本。（注意：这种功能通常被称为“远程擦除”。）
b. 拥有文档化的政策、流程和标准，当设备丢失或失窃时，能够确保对网络感知移动和便携式设备（非笔记本电脑，且存储了机密信息和个人信息）拥有物理控制权的授权个人及时删除所有的机密信息和个人信息。
c. 拥有文档化的政策、流程和标准，能够确保移动和便携式设备（非笔记本电脑和网络感知设备）在连续尝试登陆失败后会自动删除存储的所有机密信息和个人信息副本。

14.4 拥有文档化的政策、流程和标准，确保任何用于存储机密信息和个人信息的移动和便携式设备：

a. 由授权个人实际占有；
b. 未由授权个人实际占有时，确保物理安全；
c. 未由授权个人实际占有或确保物理安全时，或者在 10 次尝试失败后，立即存储其数据并安全删除。

14.5 在允许访问通过移动和便携式设备存储的机密信息和个人信息时，具备并采用一定流程来确保：

a. 用户已被授权进行该访问；且
b. 用户身份已得到认证。

14.6 实施政策，禁止使用非供应商或 CWT 管辖和/或管理的一切移动和便携式设备来访问和/或存储机密信息和个人信息。

14.7 至少每年检查一次供应商管辖或管理的所有移动和便携式设备的使用情况及控制措施，确保该设备达到适用的《技术和组织安全措施》要求。

15. 传输安全

供应商应：

15.1 在 CWT 或供应商控制的网络之外传输机密信息和个人信息或在任何不可信网络传输机密信息和个人信息时，使用强加密。

15.2 包含机密信息和个人信息的纸质、缩微胶片或经物理传输的电子介质记录，必须通过可追踪、妥善包装以及符合制造商规格的安全快递或其他运送方式进行运输。任何机密信息和个人信息都必须用上锁的容器进行运送。

16. 静态安全

供应商：

16.1 应在存储时使用强加密保护机密信息和个人信息。

16.2 不得在其网络环境（或 CWT 自身的安全计算机网络）之外以电子形式存储机密信息和个人信息，除非存储设备（如备份磁带、笔记本电脑、记忆棒、电脑磁盘等）受到强加密保护。

16.3 不得在可移动介质（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）上存储机密信息和个人信息，除非：（a）根据合同要求，用于备份、业务连续性、灾难恢复和数据交换的目的，以及（b）使用强加密。

16.4 应将包含机密信息和个人信息的记录以纸质或缩微胶片形式妥善存储保护于仅限授权人员访问的区域。

16.5 除非 CWT 另有书面规定，否则，在针对、通过或代表 CWT 或根据 CWT 品牌收集、生成或创建纸质和备份介质形式的机密信息和个人信息时，应确保该信息为机密信息和个人信息，并在条件允许时，将该类 CWT 的信息标注为“机密”。供应商承认，机密信息和个人信息始终为 CWT 拥有的机密信息和个人信息，无论是否进行标注。

17. 返还、销毁和处置

供应商：

17.1 在 CWT 的要求下，应在该要求提出三十（30）天内免费将所有机密信息和个人信息的副本提供给 CWT。不论协议是否规定，在出现以下情况九十（90）天内，供应商应返还或根据 CWT 的选择销毁所有的机密信息和个人信息（包括电子和纸质版本）：（a）当协议期满或终止、（b）CWT 要求收回机密信息和个人信息，或（c）供应商不再需要机密信息和个人信息来提供协议中的服务和产品时。

17.2 当 CWT 准许以销毁代替返还机密信息和个人信息时，应提供书面证明，确认销毁的机密信息和个人信息不可回收且不可恢复。供应商应彻底销毁存储于所有系统以及全部位置的一切 CWT 机密信息和个人信息副本，包括但不限于先前批准的供应商第三方。该等信息应根据针对彻底销毁的行业标准程序（例如 DOD 5220.22M 或 NIST SP 800-88）进行销毁，或使用制造商推荐的消磁产品对受影响的系统进行处理。在进行此类销毁前，供应商应维护所有适用的《技术与组织安全措施》，以保护机密信息和个人信息的安全、隐私和机密性。

17.3 在处置机密信息和个人信息时，应确保信息无法被重建成可用格式。纸张、幻灯片、缩微胶卷、缩微胶片和照片必须通过碎纸机粉碎或焚烧处置。包含机密信息和个人信息的待销毁材料必须存放于安全容器中，并由可靠第三方运输。

18. 保留

供应商：

18.1 均应负责在获取任何机密信息和个人信息前与 CWT 联系以验证适当的保留要求，且需符合任何工作陈述或采购订单。

18.2 应确保所有由供应商的服务、系统、设备或介质自动创建的机密信息和个人信息的所有备份副本（**“存档副本”**）得到安全保护。除非协议另有规定，否则在协议期满或终止后的 90 天或更短时间内，若 CWT 合理要求，供应商应安全销毁机密信息和个人信息的所有存档副本，遵照的行业标准程序严格程度至少相当于 DOD 5220.22M 或 NIST SP 800-88。

19. 事件响应和通知

供应商：

19.1 应具备及遵循事件管理流程，且拥有配备专门资源的相关程序和人员。一旦发现 CWT 的信息、系统或其他资源发生任何疑似或确认攻击、入侵、非法访问、丢失或其他事件，在二十四（24）小时内立即通知 CWT。

19.2 通知 CWT 后，应定时向 CWT 提供事件持续期间的最新状态（包括但不限于为解决该事件采取的行动），间隔时间或次数由双方商定；且在事件结束后尽快向 CWT 提供书面报告，详细描述事件、供应商在响应期间采取的行动，以及供应商为防止类似事件发生的未来行动计划。

19.3 如果未根据法律要求首先通知 CWT，并与 CWT 共同直接通知适当的地区、国家、州或地方政府官员，或信用监控服务、受破坏行为影响的个人，以及任何相关的媒体机构，不得在任何情况下公开披露对 CWT 信息、系统或其他资源的任何破坏。

a. 应具备一定的流程，及时发现其工作人员违反安全控制（包括本《信息安全要求》）的行为。被发现的供应商人员应依照适用法律接受相应的纪律处分。尽管有上述规定，供应商人员仍应受供应商制约。CWT 不应被视为供应商人员的雇主。

20. 业务连续性管理与灾难恢复

供应商：

20.1 应开发、操作、管理及修订业务连续性与灾难恢复计划，将 CWT 对供应商服务或产品的影响降到最低。此类计划应包括：具体针对业务连续性和灾难恢复功能的命名资源、建立恢复时间目标和恢复点目标、数据和系统的日常备份、异地存储备份介质和记录、满足协议要求的记录保护和应急预案，异地安全存储此类计划，并确保供应商可在需要时获得此类计划。

20.2 当 CWT 要求时，应向 CWT 提供文档化的业务连续性计划，确保供应商能满足协议下的合同义务，包括任何适用的工作陈述或服务级别协议的要求。在保护机密信息和个人信息的完整性和机密性时，此类计划应发挥修复作用。

20.3 应具备安全备份与恢复机密信息和个人信息的文档化流程，至少应包括运输、存储及处置机密信息和个人信息备份副本的流程，并根据 CWT 的要求提供此类文档化的流程。

20.4 应确保存储所有机密信息和个人信息的备份或 CWT 使用的系统软件和配置至少每周创建一次。

20.5 应至少定期每年一次，或在业务连续性或灾难恢复计划出现重大变化时，由供应商自己出资对此类计划进行全面演习。演习时应确保受影响的技术能够正常运作，内部人员应知晓此类计划。

20.6 应及时检查业务连续性计划，以便处理额外或潜在的威胁来源或情况，并根据要求，在合理的时间范围内向 CWT 提供高度概括的计划以及测试情况。

20.7 应确保存储或处理机密信息和个人信息的所有供应商或供应商签约地点都全天候受到监控，以防止出现入侵、火灾、水灾和其他环境危害。

21. 合规性和认证

供应商：

21.1 应将按照本《信息安全要求》和此处供应商的合规性所引起的、与其履行义务相关的完整和准确记录保留为某种格式，使其至少在三（3）年内能够被评估或审计，或根据法令、民事或监

管程序的要求持续更长时间。尽管有上述规定，供应商只需维护安全日志到持续履行协议后不少于六（6）个月。

21.2 CWT 可在不增加自身额外成本的情况下，应通过合理地提前通知，对供应商执行的《技术与组织安全措施》开展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并要求记录成文。对 CWT 的所有要求，如果适用，供应商应立即或根据双方协议以书面形式和证明作出回应。当 CWT 要求由 CWT 进行审计时，供应商应安排安全审计，且审计工作需在该要求提出后的十（10）天内开始。CWT 可要求访问设施、系统、流程或程序来评估供应商的安全控制环境。

21.3 根据 CWT 的要求，应提供遵循本文件的证明，包括最新版 PCI-DSS、ISO 27001/27002、SOC 2 的支持证明，或对供应商的类似评估。如果供应商不能证明合规，则应提供书面报告，详述未合规之处及其合规改正计划。

21.4 当 CWT 认为发生了违反安全的事件、且该事件未根据本文和供应商的事件管理流程报告给 CWT 时，应安排审计或评估，并在 CWT 要求评估或审计的通知发出后 24 小时内开始执行。

21.5 在收到评估结果或审计报告三十（30）天内，应向 CWT 提供书面报告，阐明供应商已经实施或已提出实施计划的纠正措施，以及各项纠正措施的最新执行情况。供应商应每三十（30）天向 CWT 更新该报告，报告从实施之日起所有纠正措施的执行状况。供应商应在其收到评估或审计报告九十（90）天内实施所有的纠正措施，该时间也可是双方书面约定的其他时间，但不超过自供应商受到评估或审计报告起三十（30）天。

21.6 应始终遵循政府规定的各项适用的信息安全标准、报告要求和 ISO 27001/27002 标准。处理支付账号或其他相关支付信息时，应始终遵守适用于处理该信息的整个系统的最新版支付卡行业数据安全标准（PCI-DSS）。当供应商不再符合适用于处理 PCI 适用数据的整个系统任何部分的 PCI-DSS 时，应及时通知 CWT，立即修复该不合规情况，并按照要求定期向 CWT 报告修复情况。

22. 标准、最佳做法、法规和法律

供应商：

当供应商处理、访问、查看、存储或管理与 CWT 的员工、合作伙伴、关联企业、CWT 客户，或 CWT 客户的员工、承包商或分包商有关的机密信息和个人信息时，应采用严格程度不低于国际、地区、国家、州和当地准则、法规、指令和法律要求的《技术与组织安全措施》。

23. 修改

CWT 保留不时更新或修改本《信息安全要求》的权利，并将最新版本发布在 CWT 网站上。

2.0 版本
日期：2017 年 12 月 15 日