

网络安全&信息安全与隐私保护 管理制度

最新发布日期：二〇二五年一月二十四日



版本历史变更说明

更新日期	文档编号、版本号/次	更新章节	更新内容	更新作者
2021.01.18	/	起草	起草	/
2025.01.24	QES-003-2025-A/1	新建	新建	王燕

目 录

一、 安全规划	118
1.1 目的	118
1.2 目标	118
1.3 战略方针	119
二、 管理制度	119
2.1 安全组织结构	119
2.2 安全小组职责	120
三、 网络安全 11 军规	121
四、 网络安全及隐私保护红线	122
五、 信息安全红线	123
六、 人员安全管理	124
6.1 员工资质管理	124
6.2 人员出入场管理	124
6.3 三级安全教育	124
6.4 人员安全意识提升	125
6.5 关键岗位人员管理	126
6.6 人员入离职管理	126
七、 工作便携机使用规范（安装华为系统电脑）	126
7.1 华为邮箱使用	126
7.2 工具软件来源合规	126
7.3 安装客户指定软件	127
7.4 移动存储拷贝	127
7.5 加域后安装虚拟机申请流程	128
7.6 设备硬件类故障维修	128
7.7 严重违规风险	129
7.8 外网接入内网管理（xGATE）	130
7.9 办公账号邮箱管理权限	131
八、 网络安全规范	131
8.1 法律法规	131
8.2 安全事件	132
8.3 客户安全制度	132
九、 客户网络接入管理	132
9.1 管理目标	132
9.2 实施要求	132
9.3 接入检查	133
9.4 终端病毒查杀	133

十、	客户网络数据处理	133
10.1	管理目标	133
10.2	实施要求	134
十一、	帐号密码管理	134
11.1	管理目标	134
11.2	实施要求	135
十二、	帐号密码（华为帐号）	135
12.1	申请指导	135
12.2	账号管理	136
12.3	工卡管理	137
12.4	WELINK 帐号申请	137
十三、	工程转维	138
13.1	各产品线转维清单	138
13.2	转维邮件发送要求	139
十四、	工具软件管理	140
14.1	管理目标	140
14.2	实施要求	141
十五、	备件&物料返回	141
十六、	网络安全事件处罚	142
十七、	网络安全事件处理流程	142
十八、	网络安全演练	142
18.1	网络安全演练要求	142
18.2	计划的实施保障	142

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

一、安全规划

1.1 目的

落实“网络安全和用户隐私保护”，更好地遵从法律法规和各行业的安全合规要求，建立“网络安全与隐私保护高标准的管理体系”，提升网络安全与用户隐私保护能力，规避网络安全、信息安全风险，为公司树立可信任形象，并保证网络安全&信息安全与隐私保护的要求得到有效落地。

公司网络安全管理框架—基于业务流程全方位监控管理



1.2 目标

网络安全目标

- ✧ 无重大网络安全事故
- ✧ 年度一般网络安全违规≤5 起

■ 目标释义：

● 重大网络安全事件是指在服务或生产过程中，因个人行为造成的红线违规或者一级质量事故（具体参考《问题处理与升级通报制度》文件）。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

● 一般网络安全违规是指在服务或生产过程中，因个人行为造成的二级及以下的违规或者质量事故（具体参考《问题处理与升级通报制度》文件）

信息安全与隐私保护目标

- ✧ 无重大信息安全泄露事件。
- ✧ 年度一般信息安全违规≤2 起。

■ 目标释义：

● 重大信息安全事件是指在服务或生产过程中，因个人行为造成的红线违规或者一级质量事故（具体参考《问题处理与升级通报制度》文件）。

● 一般信息安全违规是指在服务或生产过程中，因个人行为造成的二级及以下的违规或者质量事故（具体参考《问题处理与升级通报制度》文件）。

1.3 战略方针

网络安全，从我做起，是每个人的责任，也是共同守护安全的重要一环。筑牢网络安全防线，共同守护网络安全。

守护信息安全，保护用户隐私，防范于未然，筑牢信息安全底线是所有人共同的责任。

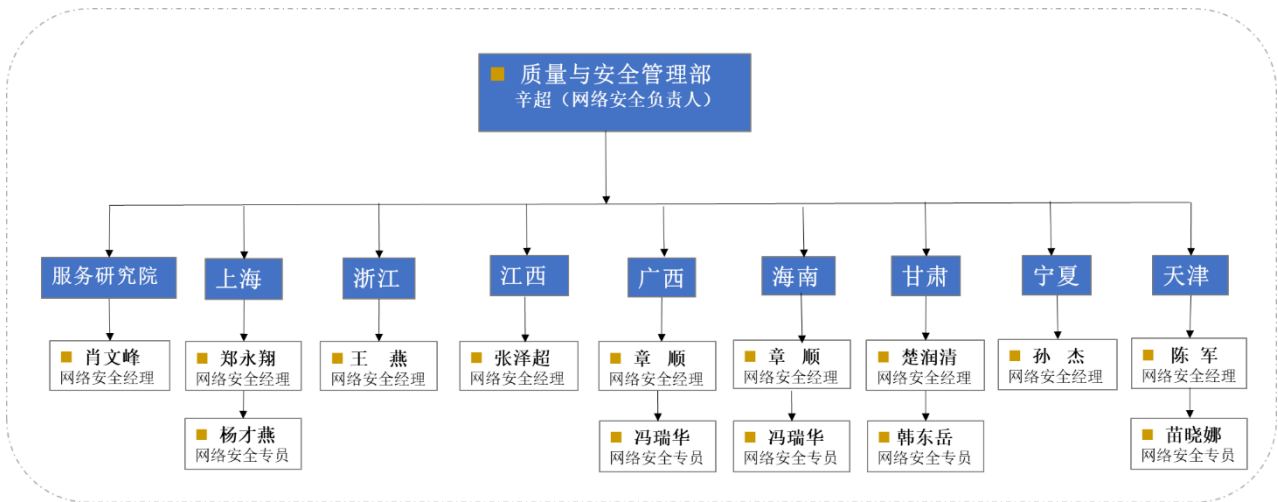
二、 管理制度

公司的安全管理包含了网络安全、信息安全与隐私保护管理。

2.1 安全组织结构

- ✧ 组织架构图

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞



✧ 安全小组人员清单

服务中心网络安全&EHS 管理组织人员清单				
序号	姓名	岗位	责任区域	职责
1	辛超	网络安全&EHS 负责人	服务中心	负责整体网络安全&EHS 体系的建设和流程制度建设
2	肖文峰	网络安全&EHS 经理	服务研究院	负责服务研究院网络安全&EHS 体系执行、落地、管理工作
3	郑永翔	网络安全&EHS 经理	上海	负责上海分公司网络安全&EHS 体系执行、落地、管理工作
4	杨才燕	网络安全专员	上海	负责上海分公司网络安全体系执行、落地、管理工作
5	王燕	网络安全&EHS 经理	浙江	负责浙江分公司网络安全&EHS 体系执行、落地、管理工作
6	张泽超	网络安全&EHS 经理	江西	负责江西分公司网络安全&EHS 体系执行、落地、管理工作
7	章顺	网络安全&EHS 经理	广西	负责广西分公司网络安全&EHS 体系执行、落地、管理工作
8	冯瑞华	网络安全专员	广西	负责广西分公司网络安全体系执行、落地、管理工作
9	楚润清	网络安全&EHS 经理	甘肃	负责甘肃分公司网络安全&EHS 体系执行、落地、管理工作
10	韩东岳	网络安全专员	甘肃	负责甘肃分公司网络安全体系执行、落地、管理工作
11	孙杰	网络安全&EHS 经理	宁夏	负责宁夏分公司网络安全&EHS 体系执行、落地、管理工作
12	陈军	网络安全&EHS 经理	天津	负责天津分公司网络安全&EHS 体系执行、落地、管理工作
13	苗晓娜	网络安全专员	天津	负责天津分公司网络安全体系执行、落地、管理工作

2.2 安全小组职责

➤ 网络安全是指在法律合规下保护产品、解决方案和服务的可用性、完整性、机密性、可追溯性和抗攻击性，及保护其所承载的客户或用户的通信内容、个人数据及隐私、客观信息流动，从而保障客户的业务连续性和合规运营，避免设备供应商、服务供应商的声誉损失及连带责任。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

➤ 网络信息安全责任人是指遵照信息安全管理体系和标准工作，防范黑客入侵并进行分析 and 防范，通过运用各种安全产品和技术，设置防火墙、防病毒、IDS、PKI、攻防技术等。进行安全建设与安全技术规划、日常维护管理、信息安全检查与审计系统帐号管理与系统日志检查等的人员。

➤ 岗位描述：

- 宣传网络安全知识，客户保密守则；
- 负责分公司整体网络信息安全管理；根据公司战略，对公司的网络信息安全体系进行整体规划；
- 梳理、评估分公司网络信息安全管理水平，推进网络信息安全管理体系建设，定期梳理优化网络安全的流程制度及相关规范要求；
- 反馈现有网络信息安全管理政策、制度与流程制定或修订的需求给公司总部；
- 监督并控制分公司网络信息安全风险，预防并处理网络信息安全事件，杜绝重大网络信息安全事故的发生；
- 负责对分公司的安全隐患地挖掘、追踪与消除；对网络信息安全问题导致的紧急与突发事件制定应急预案，并做好预防性措施及定期演练；
- 定期进行安全审计，并负责安全事件的处理、调查、报告；
- 负责分公司各种网络信息安全系统的维护和故障处理；
- 定期到现场进行网络安全稽查，输出报告；
- 负责分公司网络安全、信息安全、EHS、隐私保护等的宣传和培训工作，要求每月组织一次相关的培训。

三、 网络安全 11 军规

第一条 公司没有测试网络，测试网络就是生产网络，所有对测试网络的动网必须走变更流程！

第二条 所有非变更流程下，对现网设备（包括但不限于生产、测试、办公、监控）的登录，必须电话向 TD 和单位自有质量经理报备！

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

第三条 所有工程期间调测的网络，即使未调测完毕，一旦接入客户现网（包括但不限于生产、管理、办公、监控），即为业务生产网络，动网必须走变更流程！

第四条 公司没有删除和格式化的操作，禁止对一切设备做删除命令和格式化的操作！

第五条 登录设备前，必须确认设备名称、设备 IP 地址和相关描述，执行删除和初始化设备命令前必须进行二次确认！

第六条 落实变更方案 CheckList，所有检查项需要逐一检查核实，不能未经核实随意勾选确认检查项！

第七条 在所有现场服务中（包括但不限于交付、维护、变更、保障），只要出现任何影响了客户现网的事件，必须第一时间优先通报公司内部直接主管！

第八条 现网环境中，驻场人员，集成商不能代表客户授权！

第九条 以代表处流程为准。未经评审和未在流程内，研发提供的“现网的操作指导”“命令”，必须得到代表处 TD 的确认，才能操作！

第十条 现场操作，如果出预期外问题，5 分钟搞不定，第一时间通知 TD。

第十一条 用户名/密码单次授权获取，严禁明文传递和保存密码。实施方案和文档中不能包含用户名/密码，项目方案规划材料建议邮件单独发送，严禁微信发送。

四、 网络安全及隐私保护红线

红线一 遵守所在国相关法律法规以及客户的安全要求，确保服务过程不存在安全隐患或问题。

红线二 不破解客户的账户密码，不攻击、破坏客户网络，不窃取客户网络中的任何数据或信息。不在客户网络中植入非法代码、恶意软件或后门，不预留任何未公开接口或账号。

红线三 未经客户授权不使用非授权账号或他人账号登录客户网络进行操作。不共享账号及密码。

红线四 必须从客户指定的官方地址或通过客户提供的专用工具下载终端正式软件版本、补丁，不加载任何非官方软件。不在维修过程中引入任何形式的木马、后门、蠕虫、病毒、恶意代码、未知功能及未知权限。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

红线五 不窃取用户终端中的任何数据或信息、不破解用户的账户密码。

红线六 未经客户书面许可，不使用个人便携设备、存储介接入客户网络。

红线七 不进行超出客户定义的服务范围的任何操作。

五、 信息安全红线

红线一 必须严格遵守《中华人民共和国保守国家秘密法》及客户的相关信息安全要求。

红线二 必须严格遵守华为公司的《信息安全管理规定》及公司的相关规定。

红线三 相关业务往来邮件涉及的敏感词使用替代编码，如 GA、WA、AQJ 等。

红线四 日常工作邮件必须使用公司邮箱或华为邮箱。不得使用其他公众邮箱，特别是境外服务器的邮箱类型，如：GMAIL，YAHOO 邮箱等。

红线五 业务往来邮件中禁止出现客户网络地点、客户姓名、客户重大事件等敏感信息。

红线六 禁止在敏感场所拍照；禁止在微信朋友圈、微博等公共媒体平台发布相关内容；禁止转发、评论未经证实的非权威媒体的言论。

红线七 禁止未经客户书面授权，访问客户系统，收集、持有、处理、修改客户网络中的任何数据和信息，禁止进行超出客户审批范围内的任何操作。

红线八 禁止未经客户书面许可，使用个人便携设备、存储介质接入客户网络。

红线九 禁止使用他人账号或未授权账号登录设备进行操作。

红线十 禁止在提供的产品或服务中植入任何恶意代码、恶意软件、后门、预留任何未公开接口和账号。

红线十一 禁止攻击、破坏客户网络，破解客户账户密码；禁止泄漏和传播客户网络中的数据和信息。

红线十二 禁止未经客户书面许可，使用共享账号和密码，商用或转维后，保留或使用管理员账号及其它非授权账号。

红线十三 禁止非法软件在客户网络上运行，禁止使用来自公司非正式渠道的任何软件版本、补丁、License。

红线十四 禁止利用客户系统的信息和数据谋取个人利益或用于其它非法目的。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

六、 人员安全管理

6.1 员工资质管理

- 入职后完成网络安全上岗证考试或要求人员网络安全上岗证在有效期内（2 年）；
- 入职后手抄“网络安全及隐私保护承诺书”、“网络与信息安全承诺书”、“EHS 承诺书”、“ASP 业务服务履行质量合规承诺书”要求人员四个承诺书手抄在有效期内（2 年）。
- 从事特种作业人员，需要获取特种作业证书。如：电工证、登高证等。
- 独立操作人员必须在 iResources 中录入资源，不允许操作不符合级别的工作。

6.2 人员出入场管理

- 人员入职、驻场人员或重大项目入场需完成入场 Checklist 检查，并签署后归档；
- 人员离职、驻场人员或重大项目离场需完成离场 Checklist 检查，并签署后归档。

6.3 三级安全教育

新进公司职工（包括新调入人员、实习生、代培人员等）必须进行三级安全教育，并经考试合格后方可上岗。

- **公司级（服务中心）：**安全教育时间不少于 15 小时，其教育内容：

- a) 国家有关安全生产法令、法规和规定。
- b) 本公司的性质、经营特点及安全管理（特种信息处理及设施设备安全方面）规章制度。
- c) 安全生产基本知识、消防知识及气体防护常识。
- d) 职业安全卫生有关知识。
- e) 本公司同类型企业的典型事故及教训及有可能产生安全隐患的基础知识。

- **部门级（分公司）：**安全教育时间不少于 15 小时，其教育内容：

- a) 本单位概况，施工生产或工作特点，主要设施、设备的危险源和相应的安全措施和注意事项
- b) 本单位安全生产实施细则及安全技术操作规程。
- c) 安全设施、工具、个人防护用品、急救器材、消防器材的性能和使用方法等。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

d) 以往的事故教训。

➤ **班组级（产品线）：**安全教育由部门负责人负责培训，可采取讲解和实际操作相结合的方式进行，时间不少于 8 小时，经安全教育考核合格后，方可参与重要工作或具体任务。

a) 本岗位作业程序及工作特点和安全注意事项。

b) 本岗位安全操作规程。

c) 本岗位设备、工具的性能和安全装置、安全设施、安全监测、设备的使用和保管方法。

d) 发现紧急情况时的急救措施及报告方法。

➤ 未经三级安全教育或考试不合格者，不得分配工作，否则由此而发生的事故由分配及接受其工作单位的领导负责。

➤ **其他安全教育**

a) 对脱离操作岗位（如产假、病假、学习、外借、待岗等）六个月以上重返岗位操作者，应进行岗位复工教育。

b) 职工在公司内调动工作岗位变动工种（岗位）时，接受单位应对其进行二、三级安全教育，经考试合格后，方可从事新的工作。

c) 对严重违章违纪职工，由所在部门进行单独再教育，经考察认定后，再回岗工作。不符合工作需求的给予辞退处理。

d) 参加特殊区域、高危场所作业的人员，在作业前，必须进行有针对性安全教育。

➤ 公司和质量与安全管理部有关部门应建立安全教育、培训台帐。

➤ 安全教育工作的考核由质量与安全管理部负责，考核结果纳入公司绩效考核范畴。

6.4 人员安全意识提升

➤ 定期对服务工程师全员进行培训赋能与案例学习。（建议月度）

➤ 例行对网络变更、网络接入及数据处理、杀毒、工具软件、人员进出场管理等规范性进行自检和抽检，对违规责任人依规进行问责并及时完成问题整改。（建议季度）

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

6.5 关键岗位人员管理

➤ 识别网络安全关键人员并进行清单化管理。网络安全关键岗位是指在没有与客户流程对接情况下或有流程对接但没有客户现场陪同的情况下，可以单独接触客户关键网络节点和管理网元，并且具有足够权限 Disable 客户网络的岗位；

➤ 关键岗位人员需进行背景调查，人员更换告知客户侧关于员工岗位变动的信息；

6.6 人员入离职管理

➤ 人员入职签署保密协议，在入职后工作中对公司及客户的数据、信息有保密义务；

➤ 工作人员离岗离职之后，仍对其在任职期间接触、知悉的属于我司或者虽属于第三方但本单位承诺或负有保密义务的秘密信息，承担如同任职期间一样的保密义务和不擅自使用的义务，直至该秘密信息成为公开信息，签署《离职人员承诺书》；

➤ 离职人员离职时，应将工作时使用的电脑、U 盘及其他一切存储设备中关于工作相关或与我司会有利益关系的信息、文件等内容交接给本部门领导，不得在离职后以任何形式带走相关信息。

➤ 人员离职要按照离职人员 checklist 检查表进行检查，确保离职人员帐号、工卡、邮箱、网络数据、工作联络群等都完成清除。

七、工作便携机使用规范（安装华为系统电脑）

7.1 华为邮箱使用

➤ 电脑加域后可以申请邮箱外发权限，按实际周期申请邮件发外权限，提交主管人员进行审批。审批通过后，为确保产生违规行为，每次外发邮件时告知并抄送华为内部主管人员。

➤ 权限申请链接如下：

<https://w3.huawei.com/idaas/user/#/basic/emailPermissionOrAddressChange>

注：类似权限问题均可以进行申请

7.2 工具软件来源合规

工作便携机使用的工具软件，必须从华为合规的渠道下载安装。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

- iDesk: 本机 iDesk 客户端, 打开 “软件” 界面进行搜索
- ToolCloud (研发工具门户): <https://his.huawei.com/eportal/#/?ns=rnd>
- STM (服务工具市场): <https://stm.huawei.com/#/group/stm/search-third-tools>
- CSOP (商业软件运营平台): <https://his.huawei.com/gsam/#/toolmall>
- OSTM (开源及第三方软件管理系统): <https://ostms.rnd.huawei.com/#/portal>

7.3 安装客户指定软件

- 如因工作需要安装客户指定软件, 需要备案申请后方可使用
- 提交备案申请, 提供软件名、软件类别、备案周期, 经过业务主管审批同意, 并抄送部门信息安全专员的邮件
- 备案电子流:

<https://spa.irit-t.huawei.com/#/wf/generalFilingApply?subCategoryCode=156>

注: 代表处要按照相关安全管理规定对加域电脑进行管理, 工程师要特别注意信息安全包括但不限于:

- 未经授权, 请勿利用非标软件外传/外发公司保密信息; 如因业务需要外发需主管同意。
- 下载使用软件必须是正版软件, 不能使用盗版和破解版本。
- 使用非标软件需用公司杀毒软件进行扫描, 避免软件携带病毒、木马等风险。

7.4 移动存储拷贝

- 使用移动存储进行拷贝需严格遵守《华为信息保密管理规定 V02.10》:

<http://w3.huawei.com/pdmc/#!/core/viewDoc.html?id=355689>

- 非必须使用移动存储的情况下, 可以通过邮件外发或 eTrans 传输:

<https://etrans.huawei.com/>

注: 新版 eTrans 平台常用填单传输场景说明:

https://3ms.huawei.com/hi/group/5061/wiki_7550961.html?for_statistic_from=all_group_wiki

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

7.5 加域后安装虚拟机申请流程

- 安装非标准操作系统，需要先走备案申请流程，审批通过后再进行安装。
- 备案申请流程：

<https://spa.iright-t.huawei.com/web/securitypro/#/wf/generalFilingApply>

- 安装操作系统后，能装 xGate 的系统必须要安装 xGate。

xGate 下载链接：

<http://nshelp.huawei.com/nshelp/displayDownLoad.do?method=list>

7.6 设备硬件类故障维修

因合作方人员自带设备无华为方购买的维保，中国区驻场 IT 工程师仅提供以下协助工作，硬件设备维修/更换需求合作方自行处理。

(1) 涉数据类（如硬盘）故障：

- 由合作方人员对应的华为接口人作为信息安全担保人，由 IT 驻场当面进行便携机的硬盘拆除（三方在场：阳光雨露，华为方，合作方）；
- 由外包人员拆除下来的硬盘进行拍照，能清晰识别硬盘序列号；
- 阳光雨露当场进行物理销毁，确保硬盘处于不可再次启动/工作状态，由外包人员第二次拍照，确认硬盘序列号，确保是同一块硬盘；
- 由外包人员本人发送邮件详细说明相关事由，并将相关现场销毁的照片作为附件，发送外包方主管、华为业务接口人或其主管；
- 新硬盘到位后，需现场 IT 维护进行新硬盘的安装并安装操作系统（正版系统 license 由合作方自行提供）

(2) 除硬盘以外的其他硬件故障问题：

- 供应商接口人求助当地华为业务接口人，由他们作为信息安全担保人，由 IT 维护人员当面进行便携机的硬盘拆除（三方在场）；

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

➤ 该信息安全担保人作为硬盘保管责任人，承担维修期间硬盘信息被读取导致的信息安全风险；

➤ 送修周期较长或期间一定需要华为电脑办公的情况，可求助华为主管向 IT 或部门资产管理员，临时借一台备用电脑进行办公；

➤ 维修完毕返回后，向信息安全担保人申请取回硬盘，并由 IT 驻场当面完成硬盘的安装测试，外包人员本人将过程发送邮件给外包方主管、相关华为业务接口人或其主管。

7.7 严重违规风险

(1) 红线问题

➤ 恶意攻击、破坏客户/自营网络等通信设施，或破解客户账户密码。

➤ 在提供的产品或服务中任何环节（如研发/制造/供应/服务等）植入恶意代码、恶意软件、后门，或通过伪造、篡改发货/工程物料等方式植入后门。

➤ 未获得客户授权及指定人员的现场监督，访问或维护合法监听接口，或将相关信息传出客户网络。

➤ 非法毁损、篡改个人数据，或非法向他人或其他机构出售个人数据。

(2) 一级违规

➤ 向客户做违反网络安全与隐私保护相关法律法规的承诺，接纳违反目标市场所在国或其他适用法律要求的需求（如干扰 Disrupt，监听 Monitor，跟踪 Track 等）。

(3) 二级违规

➤ 违反公司相关规定，对外传播产品安全红线问题、产品未公开漏洞的利用信息、终端类产品的破解系统（越狱）方法。

➤ 未经客户/用户授权，访问或处理用户语音、短信、精确位置信息、按键记录等容易被质疑侵犯用户通信内容、实时跟踪用户的个人数据。

➤ 未经或超出客户/租户授权，获取、使用（存储/处理/转移/展示/销毁）客户网络、自营运网络（如云服务）中客户/租户的数据。

➤ 未经客户授权或超出授权范围接入/操作客户网络。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

- 违反公司规定，跨境转移或向第三方披露个人数据，造成实质性损害。
- 发生网络安全危机、个人数据泄露事件时，隐瞒不报或未按要求及时报告。

(4) 三级违规

➤ 违反公司规定，使用他人配置库（PDM/CC/SVN/GIT 等）帐号进行增加、修改、删除代码/文档。

➤ 接入客户网络/用户终端设备的电脑、通信终端、存储介质等未先进行杀毒，导致客户网络/用户终端设备感染或检测出病毒。

- 违反网络安全销售管控要求向客户销售产品。

(5) 四级违规

➤ 在客户/自运营网络上部署/运行来自非公司正式渠道或未经客户授权的软件版本、补丁、License。

- 在服务作业活动中，使用从非正式渠道获取或未经客户授权的服务工具。

(6) 加重场景

➤ 违规行为导致产生严重后果的，如引发法律后果、监管处罚、造成网络安全危机或 2 级以上数据泄露事件、重大客户投诉、华为公司经济损失等，可加重 1-2 级定级

7.8 外网接入内网管理（xGate）

(1) xGate权限申请

- 如应工作需要，需要从外网接入华为内网，需要申请 xGate 访问权限
访问权限开通电子流地址：

<https://w3.huawei.com/iauth/#/selectPrivilege?onlyRole=true>

- 申请需提供详细的员工信息以及对应的权限，提交申请至审批人

(2) xGate权限申请注意事项

- 公共/专业账号不能申请 xGate 权限；
- 权限有效期：默认最长一年到期，到期后重新申请；
- 新员工申请 xGate 权限，需要在入职 24 小时后提交申请。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

(3) xGate权限使用注意事项:

- 首次登陆需要进行双因子认证，请在 W3 通讯录中登记/修改手机号；
- 如若 xGate 权限到期，如需继续使用可以申请权限延期

7.9 办公账号邮箱管理权限

- 账号申请地址:

<https://w3.huawei.com/idaas/user/#/basic/accountApply>

➤ 开通“个人账户”时，根据驻场 ASP 与租赁人员管理方式相同的标准，在账号申请时默认权限需要包括：Domain（用于登入公司办公电脑、桌面云等，有该权限才能加域）、W3（用于登录公司各应用系统）、WeLink IM（收发办公即时消息）和 Email（办公邮箱），此四个权限是基础办公权限。

租赁人员权限如下图所示：

HIS

| 用户账号申请服务

首页

办公账号邮箱管理 >

域群组管理 >

账号信息查询

部门员工账号查询

我的空间 >

账号信息查询

个人账号

quhuibin 84317454

公共账号

请输入公共账号

邮箱地址

重置

	账号名	应用名	责任人	账号有效期	账号状态	账号类型
1	q84317454	Email		9999-12-31	有效	个人账户
2	q84317454	W3		9999-12-31	有效	个人账户
3	q84317454	WeLink IM		9999-12-31	有效	个人账户
4	q84317454	Domain		9999-12-31	有效	个人账户

共 4 条

八、网络安全规范

8.1 法律法规

➤ 须遵从所有的适用法律法规，包括个人数据和隐私保护、通信自由保护和网络安全保护的相关法律法规。

➤ 不得利用网络进行危害国家安全或者社会公共利益的活动、窃取或损害他人的信息、或伤害他人的合法权益。

- 不攻击、不破坏客户网络，不破解客户账号密码。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

8.2 安全事件

- 告知客户华为产品安全漏洞订阅方法，建议客户订阅（PSIRT 栏目）。若客户对产品安全漏洞有疑问，可联系 PSIRT 团队（PSIRT@huawei.com）。
- 工程师订阅华为 PSIRT 网站的漏洞预警信息，及时了解华为的漏洞信息预警及口径。
- 在获悉华为产品相关的安全漏洞时，应采取最大努力降低安全风险，并及时报告给华为（PSIRT@huawei.com），积极配合华为进行调查和处理。
- 在华为发布安全漏洞预警前，不得公开传播漏洞信息，或泄露漏洞信息给任何第三方，不得传播攻击、越狱的方法。
- 对华为发布的安全漏洞预警，合作伙伴有义务及时传递给下游客户。
- 发生安全事件时，应积极配合华为进行处理，并采取必要的补救措施。

8.3 客户安全制度

- 遵守客户的各项规章制度，遵从客户的指示及合同条款来开展服务交付活动，包括网络接入操作、个人数据处理、数据转移等；
- 进出客户机房、网管中心、办公区域、敏感区域（如政府机关、军队等）必须得到客户授权，并遵从相关管理规定。
- 使用客户电脑时接入其他网络要获取客户书面同意。如：互联网、客户业务网络、客户办公网络。
- 接入客户网络同时不允许同时接入互联网，如需接入需要单独获取授权。
- 接入检查网卡设置，必须使用客户提供 IP 地址，未经许可的 IP 地址不允许链接客户网络。

九、客户网络接入管理

9.1 管理目标

遵从客户授权，确保工程师遵从网络安全操作规范和行为红线。

9.2 实施要求

接入客户网络之前（日常维护、工程师、驻场）需获得客户书面授权（文件、短信）；

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

每次操作都遵从客户授权的要求执行（接入方式、操作行为、设备、数据类型、被授权人、时间等）。

授权书需包含以下要点：

- 1) 明确的授权人和被授权人（必选）；
- 2) 授权目的（必选）；
- 3) 授权范围：保留接入客户网络起止时间、数据处理期限（必选）；
- 4) 接入方式与发起地（如业务涉及选填）；
- 5) 接入客户网络后的操作（如业务涉及选填）；
- 6) 客户网络数据转移目的地及接收人（如业务涉及选填）；
- 7) 所访问或处理的客户网络数据的描述（如业务涉及选填）；
- 8) 客户网络数据处理完毕后的处置方式（如业务涉及选填）；
- 9) 是否涉及个人数据（如业务涉及）。

9.3 接入检查

➤ 使用客户电脑时接入其他网络要获取客户书面同意。如：互联网、客户业务网络、客户办公网络

➤ 接入客户网络同时不允许同时接入互联网，如需接入需要单独获取授权

➤ 接入检查网卡设置，必须使用客户提供 IP 地址，未经许可的 IP 地址不允许链接客户网络

9.4 终端病毒查杀

➤ 接入客户运营网络或办公网络前，接入设备（电脑/通信终端/存储介质等）要符合客户现网的网络安全环境要求和标准；

➤ 办公设备需定期进行病毒扫描和查杀，每月要有一次全盘查杀记录。

十、 客户网络数据处理

10.1 管理目标

遵从法律法规要求及客户要求，确保网络安全与隐私保护要求在数据处理等过程中合

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

规、风险可控。

10.2 实施要求

(1) 数据采集

- 1) 数据采集之前需获得客户书面授权；
- 2) 若涉及个人数据，授权中需明确个人数据的管理措施。

(2) 数据转移

- 1) 客户网络数据转移时，需遵照客户授权的范围执行（是否存在转移到非授权人的场景）。
- 2) 数据转移只允许上传华为相关业务系统或个人保留（用于日常维护），个人保留要对数据安全负责。

(3) 数据存储

- 1) 包含客户网络数据的系统/电脑/存储介质需妥善保管，严格控制访问权限。
- 2) 对于华为业务系统上传的附件默认为含有客户网络数据，数据到期后自动删除。
- 3) 客户网络数据依据谁使用谁负责的原则，保护好客户数据不被泄露，质量经理或部门主管每年对工程师保存的数据合理性进行审核。

(4) 数据使用

不允许超出客户授权范围使用客户网络数据。（如：对外交流时未脱敏等）

(5) 数据删除

- 1) 客户授权到期后，需做不可恢复的删除。
- 2) 如果客户没有明确要求删除期限，工程师处理完客户问题后，个人电脑保存的账号和密码需要在问题单关闭后90天内删除。
- 3) 工程师离开项目、维护区域或当前岗位时须彻底删除客户网络数据。

十一、帐号密码管理

11.1 管理目标

加强对服务工程师运维账号的管理，防止服务工程师因账号管控流程执行不严格，设置

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

弱口令等造成运维账号泄露，运维平台被攻击的问题。

11.2 实施要求

(1) 账号获取

登录客户网络的账号需过客户书面授权获得（短信、纸质、邮件），该授权中需明确客户网络账号使用者、使用目的及使用期限。

(2) 账号存储

账号密码不允许被明文上传到公共系统中。

(3) 账号使用

- 1) 不允许存在账号复用/共享账号，若有需获取客户书面形式授权；
- 2) 设备的初始管理员账号不允许自己保留，初始默认密码需更改。

(4) 账号清理-离职/转岗

人员离职/转岗后，以书面形式通知客户删除或修改该员工所持有的客户网络账号和密码。

(5) 密码安全性

对于新安装设备，服务工程师需及时修改密码，密码要求符合复杂度要求且未使用弱密码（如：Huawei@123、Password123!等常见弱密码）。

十二、帐号密码（华为帐号）

工程师完成iResources资源录入后，区域文员发起工号、邮箱申请。

12.1 申请指导

- 录入 iResources 系统人员必须申请华为邮箱(@mail01.huawei.com 或@huawei.com);
- 《外部人员临时通行证申请表》、《卡证办理承诺协议》盖章务必为公司公章，提供扫描件即可；
- 工卡新申请办理需要提供电子版白底正装照片，照片尺寸/大小要求：宽度不得小于 461 像素(3.9cm)，高度不得小于 579 像素(4.9cm)

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

➤ 文件大小不得大于 1MB，照片命名方式公司全称+姓名，续办不需要提供照片，（政企工卡邮箱申请表内附范本）；

➤ 工卡邮箱办理每月 1-15 号 ASP 提交申请，15 号 18:00 截止收件，申请材料邮件主送：华为工卡邮箱账号办理负责人（当前联系人：石霞 shixia3@huawei-partners.com），抄送代表处、业务部合作管理接口人。

12.2 账号管理

➤ 日常账号管理模板内所有业务 ASP 每周一统一提交申请，如遇节假日顺延，账号续期请在到期前 15 天提出申请；

➤ 日常账号管理模板只针对在有效期内的账号使用，工卡退还业务除外（反馈需求时，请整表反馈请勿截图或复制内容）；

➤ 只有 mail01 邮箱权限账号，本人无法收到系统推送的账号到期提醒，此类账号请使用人和接口人记录好账号到期时间，及时续期避免邮箱到期无法使用；

➤ 拥有 mail01 邮箱+welink/espace 权限的账号，到期提醒通过应用号推送给账号使用人；

➤ 只有 mail01 邮箱权限账号，密码重置成功后新密码以邮件形式通知接口人，拥有 mail01 邮箱+Welink/espace 权限账号密码重置成功后；

➤ 系统将以短信形式发送新密码至使用人手机；

➤ 对外发送的所有邮件必须使用后缀为@mail01.huawei.com 或 @huawei.com 邮箱；

➤ WX 账号业务办理邮件必须抄送代表处、业务部合作管理接口人；

➤ 人员离职后请在三个工作日内提出账号注销+工卡退还申请；

➤ 禁止合作方带着 WX 工号跳槽，人员离职后请及时申请账号注销，若未及时注销发生信息安全风险将向账号所属公司追责；

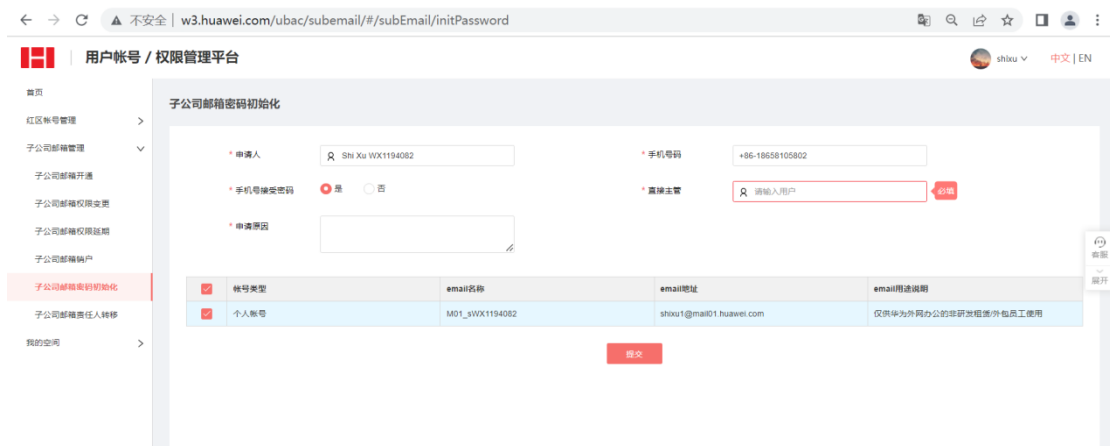
➤ mail01 邮箱在有效期内，使用人员可自行更改邮箱密码（操作流程见附件）；

➤ WX 账号相关业务办理由 ASP 备案接口人统一对接，若人员更换请邮件知会。

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

12.3 工卡管理

- 工卡有效期均为一年，到期需要续办工卡，请在到期前 60 天提交申请，收到新卡后退回旧工卡，避免出现空档期影响业务正常开展；
- 退还工卡时须按模板反馈退还工卡明细，离职退还工卡+卡绳（不需要卡壳），到期需要续办工卡只退还到期工卡即可，若未附明细出现遗漏概不负责；
- 续期工卡不再提供卡绳、名片和卡壳（第一次办理已提供，若卡绳损坏可将旧卡绳寄回更换新卡绳）；
- 通过政企地区部办理的 ASP 工卡，请退还至地区部办理人员，不可私自退还或联系他人退还，卡证丢失或在效期满 30 日后仍不归者，外部公司须赔偿华为公司安全风险费用每证 100CNY（日常账号管理模板内附罚款缴纳流程）；
- 到期工卡邮寄地址：四川省成都市郫都区天全路 200 号华为 U11，收件人：石霞 18482364003，快递要求：公司默认 EMS/顺丰。



12.4 Welink 帐号申请

工程师已有华为工号、邮箱后文员发起 Welink 帐号申请，申请帐号进行登记。

- 使用 W3 账号登录

<https://w3.huawei.com/idaas/user/#/basic/accountApply>

- 人员类型选择“外包人员”
- 申请人工号填入工程师工号；

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

- 直接主管“维护经理&服务接口人”
- 办公账号勾选 W3、WelinkPC
- 点击“提交”；

注：帐号不得互相借用、共享，离职后要及时清理

十三、工程转维

项目完工后，工程师需要对项目中产生的过程文档、设计文档、帐号密码等向客户进行移交。

13.1 各产品线转维清单

序号	产品	移交内容	是否移交	备注
备注	附件较大可线下移交，线下移交的，也要放在移交清单中，后面备注线下移交			
1	存储	LLD 规划	必选	
2		巡检报告/开局自检	必选	
3		遗留问题表	必选	
4		产品文档（可链接）	必选	
5		实施方案	可选	
6		测试文档	可选	
1	HCS	LLD 设计表	必选	
2		HCC TurnKey 工程导出表	必选	

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

序号	产品	移交内容	是否移交	备注
3		验收测试用例报告	必选	
4		用户操作手册	必选	
5		项目遗留问题报告	必选	
6		HCC Turnkey 配置表	可选	
7		概要设计	可选	
8		系统集成方案	可选	
9		项目验收方案	可选	
1	数通	LLD 规划	必选	
2		产品文档（可链接）	必选	
3		遗留问题表	必选	
4		实施方案	可选	
5		测试方案	可选	
6		巡检报告	可选	内部必须发
1	机器视觉	LLD 规划文档	必选	
2		操作指导书	必选	根据现场客户使用场景编写
3		遗留问题表	必选	
4		产品安装文档	可选	
1	数字能源	设备开机报告	必选	
2		操作指导书	必选	根据实际情况编写
3		遗留问题表	必选	
4		产品安装手册	可选	
1	其他	客户要求	可选	

13.2 转维邮件发送要求

- 附件说明：所有需要转维的材料，打包设置密码。解压密码单独告知客户
- 邮件主题：“合同名称”项目资料、帐号移交
- 发送范围：
 - ✓ 主送：客户

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

✓ 抄送：华为维护经理、华为服务接口人、华为项目经理、华为 TD、服务经理、公司项目经理、公司质量经理

4) 邮件正文

邮件正文中应包含以下内容：

- ✓ 客户人名（非客户单位名称）
- ✓ 合同号
- ✓ 合同名称
- ✓ 项目完工日期
- ✓ 移交材料/内容清单（参考上面表格）

- LLD 设计表
- HCC TurnKey 工程导出表
- 验收测试用例报告
- 用户操作手册
- 项目遗留问题报告
- HCC Turnkey 配置表
- 概要设计
- 系统集成方案
- 项目验收方案
- ✓ 移交账号清单
- 产品名称、数量、账号
- 网元名称、数量、账号

十四、工具软件管理

14.1 管理目标

必须规范使用服务工具，如果从不合规渠道获取的服务工具，通常是未经安全测试，可能存在敏感功能、后门、被植入/篡改等安全风险问题，一旦使用可能导致客户投诉甚至危

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

机事件。

14.2 实施要求

来源合规

1) 工程师必须从合规渠道获得服务工具，包括：Support网站、Support-E网站、服务工具市场、PDM产品目录、随机发货、客户提供；禁止从非合规渠道获取服务工具；

2) 研发工具市场：<http://toolcloud.huawei.com/toolmall/>

3) 服务工具市场：<http://gtstools.huawei.com/gts/>

4) Support及Support-E网站：<https://support.huawei.com/>、
<https://support.huawei.com/enterprise/>

5) ServiceTurbo Cloud工具平台：

<https://serviceturbo-cloud.huawei.com/serviceturbocloud/#/Home>

6) 使用客户提供的服务工具须满足以下条件：客户邮件等书面形式明确特定工具的使用要求（使用对象、网络、范围、期限），以及由客户提供具体的软件实体或下载地址。

十五、备件&物料返回

接收客户物料时需履行数据删除告知义务，提醒客户清除数据、确认删除部件中存储的客户数据；

文件名称	网络安全&信息安全与隐私保护 管理制度			文件编号	QES-003-2025
				版本/次	A/1
				实施日期	2025 年 01 月 24 日
编制	质量与安全管理部	审核		批准	卢晓飞

十六、网络安全事件处罚

网络安全&信息安全违规处罚标准		
违规级别	违规描述	处罚结果
红线违规	1、违反流程规范，造成一级质量事故的； 2、盗取客户物料进行盈利的 3、一年内出现2次一级违规的。	无条件解除劳动合同 情节较轻记大过，连续扣减三个月（含当月）的工资20%
一级违规	1、违反流程规范，造成二级质量事故的。 2、出现事故隐瞒通报。 3、出现客户高层投诉，对公司造成了实际影响的。（包括但不限于实际损失、声誉损失等） 4、一年内出现2次二级违规的。	记过，连续扣减二个月（含当月）的工资20%
二级违规	1、违反流程规定，造成三级质量事故的。 2、出现事故延迟通报的。 3、出现客户有效投诉的。 4、违反诚信，对于考勤、文档数据、日常反馈数据造假的。 5、无资质上岗的。	书面警告，扣除当月工资20% 情节较轻者通报批评，扣除当月工资10%
三级违规	1、客户有效投诉的。 2、违反网络安全要求的。 3、操作未进管道的。 4、满意度低于80分的。 5、导致公司绩效扣分的。	通报批评，扣除当月工资10% 情节较轻口头警告，扣除当月工资200元

十七、网络安全事件处理流程

参考《问题处理&升级通报制度》相关章节

十八、网络安全演练

18.1 网络安全演练要求

以部门为单位，建议每半年组织一次网络安全演练。

18.2 计划的实施保障

- 各部门主管提供网络安全演练脚本。
- 网络安全专员根据脚本组织演练的人员。
- 网络安全专员组织监督演练进度和结果。

EHS 安全管理制度

最新发布日期：二〇二五年一月二十四日

