软件研发中心驻场信息安全培训材料

第一章 培训目标

信息安全包括网络安全、终端安全、数据安全等方面，是企业安全和国家战略安全的一部分。通过开展软件研发中心驻场信息安全培训，有助于增强入场员工的信息安全意识，加强对网络安全、终端安全、数据安全的了解，使员工能够理解和自觉遵守软件研发中心的信息安全制度与规定。

第二章 管理现状

2.1. 总体情况

中国邮政储蓄银行软件研发中心（以下简称“研发中心”），包括 1 个总中心，4 个分中心，信息安全管理按照“属地管理”和“谁使用，谁负责”的原则，研发安全处负责研发中心信息安全统筹管理和总中心远程运维环境安全管理。总中心办公场地包括总部基地、诺德中心、永丰基地、宝坻基地等，各个基地设有安全管理员履行管理职责。

安全管理员负责各场地开发测试环境、远程运维环境的信息安全管理工作，包括：网络安全、终端安全、数据安全、场地安全、生产系统安全等。以提升信息安全水平为出发点，结合工作中的实际情况，对员工行为提出管理要求。

为确保管理要求落实到位，安全管理员在员工入场前需开展信息安全制度宣贯培训。员工入场后，安全管理员需进行信息安全巡检，及时发现违规行为，降低造成的危害，并依据《软件研发中心信息安全违规事件定级方案》对违规人员进行处罚。

2.2. 各基地情况

2.2.1. 总部基地

研发中心总部基地坐落于北京市丰台区南四环西路 188 号总部基地 16 区 21 号楼。远程运维区共有 40 个工位，需要特殊报备申请权限才可进入。

开发测试区、远程运维区的信息安全管理工作由安全管理员负责，具体情况如下：

角色	职责	对接人	联系方式
安全管理员	开发测试区、远程运维区信息安全管理	张鹏	18730930628

2.2.2. 诺德中心

研发中心诺德中心坐落于北京市丰台区樊羊路,远程运维区有工位 53 个，需要权限才能进入。

开发测试区、远程运维区的信息安全管理工作由安全管理员负责，具体情况如下：

角色	职责	对接人	联系方式
安全管理员	开发测试区、远程运维区信息安全管理	王朝	13681435519
		吴海斯	13439319557

2.2.3. 永丰基地

研发中心永丰基地坐落于北京市海淀区西北旺镇永丰基地。远程运维共 54 个工位，需要特殊申请报备方可进入。

开发测试区、远程运维区的信息安全管理工作由安全管理员负责，具体情况如下：

角色	职责	对接人	联系方式
安全管理员	开发测试区、远程运维区信息安全管理	陈保霖	18611174445
		成功	19910793117
		许白杨	89135475、15120029760

2.2.4. 宝坻基地

研发中心宝坻基地坐落于天津市宝坻区周良街道听涛路，开发测试区、远程运维区的信息安全管理工作由安全管理员负责，具体情况如下：

角色	职责	对接人	联系方式
安全管理员	开发测试区、远程运维区信息安全管理	陈君东	18920492705

第三章 信息安全要求

3.1. 网络安全基本要求

网络安全的基本属性是机密性、完整性和可用性，网络安全攻击的主要表现方式包括：中断、截获、篡改、伪造。在网络安全方面，以保护网络基础环境为主。员工应遵守以下基本要求：

1. 不得私搭、私建或扩展网络，禁止架设任何无线及有线网络接入点；

2. 任何部门和个人不得私自将 HUB、交换机、路由器、无线网卡、手机等设备接入到行内网络和计算机设备；

3. 严禁私自将笔记本等自带设备接入开发测试网或生产运维网；

4. 禁止擅自修改终端的 IP 地址、网卡 MAC 地址、网络协议、通信端口限制等参数；

5. 未经研发中心审批，严禁在基地内架设 FTP、DHCP、DNS 等服务器；

6. 未经研发中心审批，禁止监控网络流量，禁止对系统、服务器、终端、网络进行扫描、探测、侦听、攻击等任何形式的渗透活动。

7. 未经研发中心审批，禁止将开发测试终端切换至其他网络使用；禁止个人以任何形式将开发测试网设备与其他网络互联。

8. 禁止窃听网络通讯、窃取他人工作或者私人信息，禁止攻击内部计算机或其他网络设备。

3.2. 终端安全基本要求

终端设备包括台式机、瘦终端、专用设备等。在终端安全方面，以防病毒为主，同时涉及身份认证、终端设备管理等内容。员工应遵守以下基本要求：

1. 计算机终端使用人员必须定期更改用户登录密码，应强口令密码，8 位以上包括数字、

大小写字母、特殊字符，且不带有词组句子规律和键盘规律。

2. 终端需开机密码和超时锁屏功能，屏保启动时间不多于 3 分钟且需要输入密码解锁。临时离开工位须锁屏，离开场地须登出终端或关机，防止他人未经授权使用。

3. 软件研发中心统一要求部署终端防病毒软件是天擎，使用时需进行准确的资产登记。如果办公电脑未安装，应主动安装天擎软件，不使用未安装天擎软件的电脑进行办公。

4. 更换新的终端后，设置天擎策略须向研发安全处进行备案登记。

5. 严禁在终端上连接其他任何设备或为任何设备充电，包括非生产运维安全优盘、手机、无线网卡、耳机、充电宝等。

6. 任何人如果发现疑似中毒、被远程操控等异常情况，需立即断网、关机，并及时向信息安全管理部门反馈，并配合做好处置工作。

7. 国产化设备需按照正常终端安全要求进行日常入网、使用等。

8. 因工作需要在开发测试终端上开放数据拷贝接口或连接外设（如高拍仪、指纹仪、读卡器等）的，需经开发研发中心审批，且每次申请使用期限不得超过 12 个月。

9. 开发测试终端不得带出开发测试场地，因特殊原因确需带出的，需经开发测试环境使用单位审批，落实设备保管责任。

10. 我行配发的和非本单位人员经审批带入开发测试场地的计算机设备不得进行与开发测试相关的代码编写、系统测试等工作，严格禁止脱离开发测试网络环境开发、测试。

11. 使用人员应确保开发测试终端上安装使用的软件程序的合法、合规性，不得安装的软件程序包括（但不限于）：盗版软件、外部获取未经我行授权的软件、远程控制软件（向日葵、TeamViewer 等）、带有黑客行为的软件（如：扫描、嗅探、漏洞利用工具等）及与工作无关的其它软件等。

12. 不得自行修改安全管理软件下发的主机防护策略，应定期开展包括防病毒扫描在内的主机安全扫描，且扫描过程不可取消。

13. 对开通互联网的终端进行重点安全监控，及时发现并处置安全事件。

3.3. 数据安全基本要求

数据的流转过程通常包括数据的收集、存储、使用、加工、传输、提供、公开等。在数据安全方面，防止数据泄露是核心。员工应遵守以下基本要求：

1. 在终端上进行数据拷入时，必须使用行方统一制作的安全 U 盘；

2. 工作中的敏感信息文档需要妥善保管，不能随意放置；

3. 禁止将软件研发中心的重要文档保存在自己的电脑和私人 U 盘上；

4. 不可以以任何形式或方式传播公司未公开的信息，公司资料禁止随意拷贝、禁止在微信或其他群组中上传，禁止打印公司商密文件给其他人传阅。

5. 终端与终端间转网的数据需报告研发安全处进行数据清退。

6. 数据拷入、拷出开发测试环境需审批登记。

7. 生产环境数据导入开发测试环境前，必须经不可还原的脱敏处理。

8. 严禁拷入涉密的数据、未脱敏的生产数据、盗版软件、外部获取未经我行授权的软件、远程控制软件、带有黑客行为的软件及可能对开发测试环境产生威胁的软件，严禁以加密等方式绕过安全工具扫描。

9. 使用移动存储介质存储传递开发测试数据，应采用磁盘加密、文件加密等加密技术保护数据。在使用移动存储介质完毕后，应及时将其格式化，不得保留相关数据。当利用移动介质与非邮储银行人员进行数据交换时，必须在交换前将介质内的原有内容有效清空，并当面进行数据交换，数据交换完毕后立即收回移动存储介质。

10. 纸质存储和传递的开发测试资料应妥善保管，销毁时需用碎纸机或其他完全性销毁

手段进行销毁。

11. 邮储银行开发的信息系统的项目过程文档、源代码、测试数据等开发测试数据均属于我行数据资产，未经我行书面许可任何人均不得私自外泄至百度网盘、GitHub 等互联网平台。源代码、拓扑图、批量项目过程文档等敏感信息，禁止脱离开发测试环境存储

3.4. 开发测试区安全要求

1. 所有人员都应佩戴员工门禁卡或临时通行证，不得转借，不得进入非授权区域。当发现非本单位人员无人陪同时，应向开发测试环境所属安全管理部门报告。

2. 非本单位来访人员需登记，确保其有本单位行方员工陪同，方能允许进入开发测试场地。

3. 进出开发测试场地各区域需确认门禁锁闭到位，防止尾随，禁止敞开重要区域门禁，禁止为没有权限的人员开门。

4. 使用远程访问开发测试网络和系统时，严禁处理涉密文件以及包含客户敏感信息的数据。

5. 新增设备接入开发测试网需向资源环境测试处进行报备，开通 U 口需向研发安全处进行申请。

6. 如有互联网访问需求的，需向研发安全处申请开通转网。

3.5. 远程运维区安全要求

1. 除研发中心行员之外的人员申请远程运维区门禁权限，按照“一事一议”的原则，提交信息安全管理处室审核，提请部门负责人审批。

2. 所有进入远程运维区人员须报备安全管理处室进行审核，并在进入时按照要求进行登记，不得尾随他人进入远程运维区。

3. 研发中心行员之外的人员进入远程运维区需有研发中心行员全程陪同，不得在远程运维区单独操作运维终端。

4. 进入远程运维区须随手关门，不得使远程运维区门禁处于常开状态（消防、防疫等临时管控期间除外），不得放任尾随人员进入远程运维区。

5. 严禁在远程运维场地从事与生产运维无关、影响他人工作或破坏工作秩序的事情，如扎堆闲聊、打架斗殴等。

6. 严禁长时间占用远程运维终端，当远程运维区人数达到场地内最大工位数时将进行限流管控，各使用处室应按照实际需求报备给安全管理处室审批。

7. 严禁将笔记本电脑（包括 PAD 等）带入远程运维场地，确需将笔记本电脑带入远程运维场地的，需由行方人员向研发安全处申请，批准后方可带入。

8. 严禁在运维终端上使用非加密移动存储设备，使用加密 U 盘时应先用安全管理软件进行病毒扫描。

9. 严禁卸载或退出运维终端安全管理软件，严禁私自修改运维终端安全管理配置，包括通过修改注册表等强制方式修改安全管理配置。

10. 严禁运维终端开启文件夹共享功能。

11. 严禁在运维终端安装和使用盗版软件，运维终端安装应遵循“最小安装”原则，禁止安装与工作无关的软件。

12. 严禁在远程运维区通过拍照、录屏、抄写等方式记录并传输生产系统源代码、数据库、日志等敏感信息。

13. 严禁在运维终端上存储敏感信息（包括但不限于客户信息、源代码等），临时使用后应及时清除。

14. 生产系统账号密码应妥善保管，严禁通过记录张贴、系统自动保存密码等方式泄露密码。

15. 不得将涉及敏感信息、保密信息的纸质文件、存储设备等载体遗留在远程运维区。

3.6. 其他要求

1. 人员入场后应当深入了解并严格遵守研发中心信息安全管理制度，对于没有遵守规定的人要制止并举报；

2. 如果遇到项目经理要求做的事情与制度不符的情况，应主动向项目经理说明这样做违规；

3. 外协人员笔记本电脑需要申请备案并下发入网签且贴好，才可以带入基地使用，仅可以用于日常办公处理文档；

4. 外协人员笔记本电脑、行员的第二台笔记本电脑、标签已过有效期的笔记本电脑必须经过备案方可带入办公区使用（指进入各场地）；

5. 在使用电子邮件时，不随意打开电子邮件附件中的可执行文件，如 exe、bat 等，不随意点击陌生人邮件中的链接；

6. 禁止使用盗版软件，使用盗版软件属于违法行为，盗版软件已经成为计算机病毒的重要来源和传播途径之一，可能会包含不健康的内容；

7. 安全 U 盘、堡垒机 ukey 应当随身携带，避免丢失；

8. 申请开通互联网的终端需进行安全扫描，中、高危安全漏洞完成修复后才能开通相应访问权限。开通访问权限后如发现新的中、高危安全漏洞需立即暂停权限，待修复完成后方可重新开通。

第四章 违规处理流程

4.1.1. 违规处置

研发安全处发现违规行为，通知厂商现场安全责任人、行方管理人员配合调查。违规行为包括：在工作中存在违反研发中心信息安全管理相关制度的行为；对我行信息系统、设备设施等造成损坏，对合规管理、工作秩序等产生不良影响；给我行带来潜在的信息科技风险、法律和声誉等风险；未按保密要求对相关材料进行妥善保管、已经泄露或存在泄露风险；根据现场情况认定有主观故意情节，多次告警仍然违反相关规定、不配合安全管理员管理工作、情节严重等。

信息安全要求	处置措施
网络安全 终端安全 开发测试区安全	1. 现场责令整改，通知行方管理人员和厂商安全责任人配合调查； 2. 暂扣涉事终端做进一步安全扫描和备份登记； 3. 违规人员须重新接受研发安全处组织的信息安全培训和考试； 4. 涉事终端在违规人员考试合格后，经厂商现场负责人、处室负责人签署违规物品领回单后方可领回。
数据安全	1. 通知行方管理人员和厂商安全责任人配合调查； 2. 调查完毕现场责令删除带有敏感信息的文字或图片； 3. 对涉事终端或设备文档进行扣留及追溯，做进一步的安全扫描和备份登记； 5. 违规人员须重新接受研发安全处组织的信息安全培训和考试； 4. 违规人员考试合格后，经厂商现场负责人、处室负责人签署违规物品领回单后方可领回。
远程运维区安全	1. 通知行方管理人员和厂商安全责任人配合调查；

	2. 调查完毕后责令违规人员离开远程运维区； 3. 违规人员须重新接受研发安全处组织的信息安全培训和考试； 4. 违规人员考试合格前不得报备进入远程运维区。

4.1.2. 事件定级

对于行内发现的违规事件，综合各要素对信息安全事件进行定级，如果出现不同要素定级不一致的情况，按就高原则定级。当主体年度内累计违反同一级别信息安全管理规定达到 3 次，从第三次定级开始在前一次基础上提升 1 级，最高达到五级。在 HW、重保、监管检查等特殊时期，信息安全违规事件定级提升 1 级，最高达到五级。（可参考附录 7.1 常见违规事件分类和定级）

参考要素 事件定级	事件影响	潜在风险	信息密级	主观意志	举例
一级	轻微	较低风险	工作秘密	疏忽大意	遗失 ukey、进入生产区不进行登记、遗留 UKEY 等设备在远程运维场地等；
二级	一般	低风险	普通商密、生产系统工单	间接故意	放任或尾随他人进入远程运维区的、未经报备批准私自进入远程运维区、未经批准将笔记本电脑（包括 PAD）等设备带入研发中心并使用、泄露我行生产系统工单等材料、未妥善保管 ukey 等重要设备导致丢失的；
三级	中度	中风险	生产系统重要数据		多次提醒不登记或伪造登记信息的、伪造远程运维区登记信息或登记信息不完整清晰、私自将未安装天擎的电脑等不满足基础安全条件的设备接入行里网络环境、私自通过改变或切换终端设备的网络设置，私自搭建 Wifi 或收集热点扩展网络、泄露我行信息系统重要数据等，包括但不限于非核心源代码、日志、架构文档、设计文档等，终端或云桌面安装与业务或工作无关的软件或使用盗版软件；
四级	严重	高风险	敏感信息	直接故意	私自利用行里网络开设游戏网站、论坛、聊天室等与工作无关的网络服务，未按规定执行防病毒措施，未及时修补漏洞等造成网络和病毒攻击的，泄露我行敏感信息，包括但不限

					于客户敏感信息、账号密码等个人隐私数据、可能对行里的信息系统安全产生影响或造成微信的数据等，私自修改系统安全配置或安全管理软件培训，强制关闭或卸载天擎安全管理软件等；
五级	特别严重	较高风险	核心商密		绕过网络安全管理对远程运维环境或开发测试环境进行扫描、攻击等渗透活动，利用系统漏洞、系统权限或生产环境从事非法活动或获取私利的，泄露包含我行核心商密的材料等。

4.1.3. 处罚手段

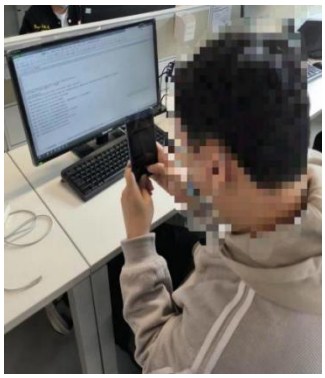
研发安全处按照事件调查报告和职责分工认定主要责任，并依据处罚规则提出处罚意见，主要的处罚措施包括警告、通报、约谈、离场，考核和经济处罚等，处罚的主体包括行员、外协外包、违规人员所在处室、供应商，具体处罚措施将依据违规事件定级和情节的严重程度进行议定。

事件级别 主要责任方	**行员**	**外协外包**	**用人处室（同内控合规指标）**	**人力外包供应商**	**项目外包供应商**
一级	警告	警告	每起扣处室绩效不低于0.05 分	对厂商安全责任人进行警告	每起事件扣供应商考核不低于 1 分（依据项目外包供应商管理实施细则考核评分方法中的相关扣分项执行）
二级	通报	通报	每起扣处室绩效不低于0.1 分	对厂商安全责任人进行通报	每起事件扣供应商考核不低于 2 分（依据项目外包供应商管理实施细则考核评分方法中的相关扣分项执行）
三级	约谈,每起扣除个人绩效不低于0.5 分	约谈，取消当年评优资格	每起扣处室绩效不低于0.5 分	每起罚款不低于5000 元（依据人力外包供应商管理实施细则第四十六条 其他处罚依据邮储银行及研发中心相关管理 规定执行）	每起事件扣供应商考核不低于 3 分（依据项目外包供应商管理实施细则考核评分方法中的相关扣分项执行）
四级	约谈，每起扣除个人绩效不低于0.8 分	约谈，年底考核结果 B 以下，取消当年晋升资格	每起扣处室绩效不低于 1 分	每起罚款不低于20000 元（依据人力外包供应商管理实施细则第四十六条 其他处罚	每起事件扣供应商考核不低于 4 分（依据项目外包供应商管理实施细则考核评分方法中的相关扣分项执行）

				依据邮储银行及研发中心相关管理 规定执行）	
五级	约谈、每起扣除个人绩效不低于 1 分	责令离场，扣除不低于 22 人天费用	每起扣处室绩效不低于 2 分	责令违规人员离场，每起罚款 22 人天且不低于 30000 元的费用（依据人力外包供应商管理实施细则第四十四条 外包服务人员违反研发中心信息安全管理规定经研发中心科技风险专题会定级为五级的，要求违规人员离场，并且扣除供应商相应级别至少 22 人天费用）	责令违规人员离场，每起事件扣供应商考核不低于 5 分（依据项目外包供应商管理实施细则考核评分方法中的相关扣分项执行）

第五章 案例介绍

2022 年 3 月中旬，某项目组开发人员李某（化名）因排查程序问题，在同事的要求下，企图将日志信息拍照并通过微信传输。此举违反了《中国邮政储蓄银行软件研发中心远程运维环境安全管理实施细则》第二十七条：“**严禁在远程运维区通过拍照、录屏、抄写等方式记录并传输生产系统源代码、数据库、日志等敏感信息**”。安全管理员发现后，按照违规处理流程对事件进行处置。



事件发生后，安全管理员现场制止员工违规行为，防止事件影响范围扩大。同时，向行员、厂商项目经理通知事件情况，要求其前往现场协助配合事件调查。通过现场取证、会谈等方式，安全管理员完成现场调查工作，形成调查报告，同时责令违规人员删除带有敏感信息的文字或图片，防止敏感信息泄露。

由软件研发中心信息安全管理委员会对违规事件定级，在事实情况调查清楚的情况下，议定划分责任、评估事件影响和风险。综合考虑相关因素后，该将起事件定为 4 级。考虑行员、用人处室、供应商已经尽到安全管理责任，因此由违规人员承担事件的全部责任。

依据事件定级、责任划分结果，由风险专题会议定处罚手段。由研发安全处对李某进行约谈，取消其当年在行内的评优资格。约谈后，该公司取消了李某当月的绩效奖金以及年度评优资格。除上述处罚外，李某需**重新参加培训**，**考试合格方可使用远程运维环境**。

此外，安全管理员还可通过视频监控等手段，发现远程运维环境中的违规行为，并对违规人员予以追责。

第六章 考试事项

6.1. 考试要求

1. 培训后必须参加考试，否则禁止使用开发测试环境和远程运维环境；
2. 入场人员考试成绩达到 70 分及以上，或补考成绩达到 80 分及以上视为考试合格；
3. 重新参加培训人员考试或补考成绩达到 90 分及以上视为考试合格；
4. 考试不合格者禁止使用开发测试环境和远程运维环境并重新参加培训。

6.2. 考试安排

1. 考试方式

使用邮问易答系统进行线上考试，考试链接、考试时间等信息将在考试前通知厂商负责人。考生登录后在右上角个人图标里点击“我的考试”，即可看到推送的考试。

考试时通常使用邮问易答系统的互联网接口，考生需要使用身份证号、手机号登录。在 HW、重保等特殊时期，邮问易答系统考试功能将暂停，入场考试以研发安全处备用考试链接为主，将在考试前向厂商负责人通知。

2. 时间安排

试卷作答时间为半个小时，包括单选、多选、判断等题型。研发安全处将根据培训、考试情况确定考试、补考的开放时间，在开放时间内考生可自行安排时间参加考试。

3. 人员组织

研发安全处将根据培训名单推送考试，推送前会将名单交由厂商负责人进行核对。厂商负责人、培训人员务必确保所填信息的准确性，以免考生无法考试。如个别人员因故缺考，请厂商负责人及时向研发安全处说明情况，以免影响入场。

4. 常见问题

a. 如果看不到推送的考试，请与安全管理员联系，确认考试是否推送成功；

b. 如果考试过期无法参加考试，请与安全管理员联系，参加补考。

第七章 附录

7.1. 常见违规事件分类和定级

分类	事件描述	违反规定	事件定级
场地安全	阻挡或敞开远程运维区门禁	严禁远程运维场地门禁常开、出入随手关门，防止尾随	二级
	放任尾随人员进入远程运维区而未加以制止		二级
	进入远程运维区不登记	进入远程运维区必须要登记	一级
	进入远程运维区经多次提醒后仍不登记		三级
	伪造远程运维区登记信息或登记信息不完整清晰		三级
	将本人门禁卡转借他人使其进入远程运维区	远程运维区门禁卡不得转借	二级
	未经报备批准私自进入远程运维区	行员之外的人员进入研发中心非授权区域需要研发中心行员全程陪同	二级
	行员之外的人员没有研发中心行员陪同私自进入远程运维区		二级
	未经批准将笔记本电脑（包括 PAD）等设备带入研发中心使用	严禁将未经批准笔记本电脑（包括 PAD 等）设备带入远程运维区场地	二级
	在远程运维区从事与运维工作无关、影响他人工作或破坏工作秩序	在远程运维场地不得从事与运维工作无关、影响他人工作或破坏工作秩序的事情	三级
系统网络安全	私自将未经批准的电脑、手机等设备接入行里网络环境	严禁将不满足基础安全条件的设备接入生产运维或开发测试环境，严禁利用邮储银行网卡开设与工作无关的网络服务	三级
	私自将未安装天擎的电脑等不满足基础安全条件的设备接入行里网络环境		三级
	私自利用行里网络开设游戏网站、论坛、聊天室等与工作无关的网络服务		四级
	私自通过改变或切换终端设备的网络设置，私自搭建 Wifi 或手机热点扩展网络	不得私自将设备接入网络，不得私自改变终端设备的系统和网络设置，严禁私自搭建或扩展网络，须按规范执行防病毒措施、严禁从事危害网络安全的活动	三级
	未按规范规定执行防病毒措施或未及时修补漏洞等造成网络和病毒攻击的		四级
	绕过网络安全对远程运维环境或开发测试环境进行扫描、攻击等渗透活动		五级
	利用系统漏洞、系统权限或生产环境从事非法活动或获取私利的		五级
信息数据	遗失或泄露我行工作秘密等材料	须按规定落实网络安全和数据安全要求	一级
	遗失或泄露我行普通商密、生产系统工单等材料		二级

安全	遗失或泄露我行信息系统重要数据等，包括但不限于非核心源代码、日志、架构文档、设计文档等		三级
	遗失或泄露我行敏感信息，包括但不限于含客户敏感信息、账号密码等个人隐私数据、可能对行里的信息系统安全产生影响或造成威胁的数据等		四级
	遗失或泄露包含我行核心商密的材料等		五级
	在终端设备存储敏感信息（包括但不限于含客户敏感信息、账号密码等个人隐私数据、可能对行里的信息系统安全产生影响或造成威胁的数据等）未及时清除	敏感信息须妥善保管、严禁敏感信息外泄互联网平台	三级
	远程运维区通过录屏、拍照、抄写等方式记录我行系统设计文档、源代码、数据库、日志等敏感信息并造成互联网传播		四级
	未按规定查阅、浏览、拷贝、打印敏感信息或数据		四级
	生产系统使用保存密码、自动登录等功能	严禁泄露或盗用帐号和密码信息	二级
	张贴帐号和密码信息		三级
	未经授权擅自使用、盗用他人用户号登录系统操作		四级
设备设施安全	终端、云桌面等未设置登录密码或弱口令	终端、云桌面等应设置开机口令和屏幕保护程序，且必须满足密码复杂度要求	二级
	离开工位未登出或锁定终端、云桌面（3 分钟未自动锁定的）	临时离开工位须锁屏、长时间离开工位须登出、离开运维场地须关机	二级
	离开远程运维区终端未关机		三级
	终端等设备未进行实名资产登记或病毒库过期	终端应安装我行终端安全管理软件，不得私自修改安全管理软件配置、不得关闭或卸载安全管理软件	三级
	强制关闭常驻内存的远程运维终端或云桌面安全管理软件进程		四级
	私自修改系统安全配置或安全管理软件配置		四级
	强制关闭或卸载天擎安全管理软件		四级
	终端或云桌面安装与业务或工作无关的软件或使用盗版软件	终端禁止安装与工作无关的软件，应遵循“最小安装”原则。	三级
	终端开启文件夹共享功能		二级
	未妥善保管 ukey 等重要设备导致丢失	堡垒机 UKEY 和生产运维安全优盘须妥善保管，离开工位时须带走，不得随意丢弃	二级
	遗留 UKEY 等设备在远程运维场地		一级

说明：

1、以上违规事件的定级仅供参考，实际定级需按照定级要素综合评定、并以风险专题会审议结果为准。

2、研发中心违规事件包括但不限于以上所述的，凡对研发中心信息安全产生影响或带来风险的事件都需要进行定级。