保密与信息安全管理制度

第一章 总则

第一条 目的与依据

为规范北京维康慈善基金会（以下简称“基金会”）的信息安全与个人数据处理活动，保障基金会信息系统稳定运行，保护捐赠人、受益人、合作伙伴、员工及其他相关方的合法权益，防范信息泄露、篡改、丢失及滥用风险，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《慈善组织信息公开办法》等相关法律法规及基金会章程，特制定本制度。

第二条 适用范围

本制度适用于基金会全体工作人员（含正式员工、实习生、志愿者）、理事会成员，以及所有访问、处理基金会信息资产和数据的外部合作方、供应商。

第三条 核心定义

（一）信息资产：指基金会拥有或控制的，以电子或非电子形式存在的数据、软件、硬件、服务、人员及其承载的信息。

（二）敏感数据：包括但不限于：

1.个人信息：以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

2.重要业务数据：未公开的捐赠记录、项目文件、财务数据、内部决策文件、尚未公开的审计报告等。

核心管理数据：员工人事档案、薪酬信息、系统账号密码、密钥等。

1.数据处理：包括数据的收集、存储、使用、加工、传输、提供、公开、删除等。

第四条 管理原则

基金会信息安全与数据处理遵循以下原则：

1.合法合规原则：所有活动必须严格遵守国家法律法规和监管要求。

2.权责一致原则：明确信息安全责任部门及岗位职责，建立责任追究机制。

3.目的明确与最小必要原则：数据收集、使用应有明确、合理的公益目的，并限于实现处理目的的最小范围。

4.安全保障原则：采取与技术风险等级相适应的管理措施和技术手段，确保数据安全。

5.公开透明原则：依法依规公开数据处理规则，保障相关方的知情权。

第二章 组织架构与职责

第五条 信息安全与数据保护工作小组

基金会设立信息安全与数据保护工作小组，由秘书长担任组长，成员包括各部门负责人及综合部负责人。其主要职责为：

1.审议批准信息安全与数据保护策略、制度。

2. 监督、检查本制度的执行情况。

3. 协调处理重大信息安全事件与数据泄露事件。

4. 组织开展全员信息安全意识培训。

第六条 各部门职责

1. 秘书处：作为主责部门，牵头制度修订、日常监督、审计与培训；负责物理安全、档案管理。负责与相关技术层面安全防护对接，包括网络、系统、终端的安全运维，实施技术措施，应对技术类安全事件。

2. 业务部门（项目部/对外合作部）：负责本部门业务范围内数据收集、使用的合规性，落实数据安全要求，管理业务系统账号权限。

3. 财务部门：负责财务数据与系统的安全。

4. 全体员工：严格遵守本制度，对其接触、处理的信息和数据负有安全保密责任。

第三章 信息资产管理

第七条 资产识别与分类分级

基金会定期对信息资产进行盘点，并依据数据敏感性、重要性进行分类分级（如：公开、内部、机密、绝密），并实施差异化保护。

第八条 物理与环境安全

1. 重要服务器、网络设备应放置在专用的、受控的机房环境。

2. 办公区域应设置门禁或访问控制，防止未经授权的物理进入。

3. 含有敏感信息的纸质文件应存放在上锁的文件柜中，废弃文件须使用碎纸机销毁。

第四章 数据处理全生命周期管理

第九条 数据收集

1.收集个人信息，须以清晰、易懂的方式告知信息主体收集的目的、方式、范围、保存期限及权利行使方式，并取得个人单独同意（法律另有规定除外）。

2.不得收集与项目或活动无关的个人信息。

3.通过合法、正当渠道获取数据，禁止窃取或非法购买数据。

第十条 数据存储与使用

1.敏感数据应加密存储。存储个人信息的系统应具备访问控制、操作日志等功能。

2.数据访问遵循“最小权限”原则，员工只能访问其职责必需的数据。

3.严格限制批量导出、复制敏感数据。确因工作需要的，须经部门负责人及信息安全工作小组审批。

4.数据使用不得超出收集时声明的目的范围。如因新的公益目的需扩大使用范围，应重新取得同意或进行合规性评估。

第十一条 数据加工与共享

1.在进行数据匿名化处理时，应采取技术措施确保数据无法被重新识别。

2.原则上不对外共享或转让敏感数据。确需向审计机构共享的，必须:

- 进行安全影响评估;

• 事先告知信息主体并征得其单独同意（法律、行政法规另有规定的除外）。

• 签订保密及数据处理协议，明确双方责任;

第十二条 数据公开

1.按照《慈善组织信息公开办法》等要求，依法依规在指定平台公开募捐情况、项目进展、财务报告等。

2.公开信息前，须进行内容审核，防止泄露捐赠人、受益人不同意公开的个人信息或隐私。

3.公开年报、审计报告时，如需披露案例，应进行匿名化处理。

第十三条 数据删除

1.当存储期限届满、处理目的已实现，或信息主体撤回同意时，应主动删除个人信息。

2.删除操作应确保数据不可恢复。对存储介质进行报废处理时，需进行数据彻底清除。

第五章 技术安全措施

第十四条 网络安全

1.办公网络与互联网边界部署防火墙、入侵检测设备。

2.核心业务系统与办公网络进行逻辑或物理隔离。

3.员工远程访问内部系统须通过安全VPN。

第十五条 系统与终端安全

1.所有办公电脑必须安装指定的防病毒软件，并及时更新。

2. 操作系统、应用软件定期安装安全补丁。

3. 禁止使用未经授权的软件和移动存储设备。

4. 移动设备（笔记本电脑、手机）处理工作数据时，必须设置屏幕锁和存储加密。

第十六条 身份认证与访问控制

1. 重要系统采用用户名/密码双因素认证。

2. 员工离职或转岗，综合部应及时禁用或调整其系统权限。

第六章 安全事件管理与应急响应

第十七条 事件定义与分类

信息安全事件包括：网络攻击、系统瘫痪、感染病毒、数据泄露、数据丢失、内部违规等。

第十八条 报告与处置流程

1. 任何人员发现安全事件，须立即报告部门负责人及秘书处。

2. 秘书处立即采取隔离、断网、备份等初步措施，防止事态扩大。

3. 工作小组评估事件级别，启动应急预案。涉及个人信息泄露的，须在法律规定时限内向主管部门报告，并通知受影响的个人。

4. 事后进行根源分析，整改问题，追究责任，完善制度。

第七章 其他

第十九条 附则

1. 本规范由基金会财务部负责解释与修订。

2. 本规范于第二届理事会第八次会议审议通过。

3. 本规范于审议通过之日起生效。