新员工信息安全学习&承诺书

1. 信息安全防护要求

一、加强个人电脑安全防护

1、个人电脑关闭远程登录访问功能，不使用向日葵、todesk、VNC等远程登录软件，不使用未经授权的VPN，禁止在办公网环境下使用个人电脑连接 VPN；

2、安装杀毒软件，做好病毒查杀、补丁升级和系统加固工作；

3、设置电脑显示文件后缀名，不随意点击外网不明来源邮件，不点击陌生人发送的exe程序；

4、在使用公共网络（如机场、酒店等场所的网络）处理公司业务时，务必通过公司 VPN 进行安全连接，并确保数据传输加密。

二、注意防范钓鱼邮件

1、提高警惕、克服麻痹思想，**注意防范钓鱼邮件**，对提供了“链接”、“密码”和“附件”的邮件，务必提高警惕，不要轻信发件人地址中显示的“显示名”，要**仔细识别发件邮箱全称**，不要轻易点开陌生邮件中的链接或附件文档；特别是使用windows系统电脑尤其注意不要打开.exe文件。

2、公司内部微信群、飞书群新增人员，或新添加微信好友、飞书好友等，要对人员身份进行严格鉴别，如果发现群内成员或者陌生人员存在发送恶意程序、恶意链接等异常行为，及时上报。

3、公司内部发布的各类通知都会提供相关负责部门联系人的公司办公电话及公司内部邮箱，对未提供公司办公电话或内部邮箱联系方式的通知，要尤其警惕，以防上当。

4、警惕通过其它发件箱发布的任何有关邮箱账号密码修改、存储空间扩容等邮件通知。

附：钓鱼识别与防护

三、杜绝弱口令

1、**杜绝所有账号的弱口令、空口令情况**；

2、密码必须包含大小写字母、数字、特殊符号，至少10个字符，避免使用出生日期、电脑键盘连续字符作为密码；

3、**本地、飞书文档中不保存明文账号和口令**。

四、提高安全意识

1、离开工位锁屏，**下班关机、断网**；

2、不访问与工作无关网站及不可信的网站；

3、不分享账号、门禁等权限资源及相关信息；

4、关于攻防演练相关信息仅限在公司内部网络交流，严禁在论坛、微信、微博等互联网平台上发布、传播本专项行动相关信息。

五、应急处置

1、如发现办公网存在安全隐患或遭受网络攻击，**请立即断开网络连接**，并第一时间联系运维安全部，同时配合运维安全部进行处置工作。

2、在专项保障活动期间，若发现信息、数据安全相关事件，请及时联系运维安全部。

六、违规处理

在此期间，如因个人原因导致出现被上级单位认定的信息和数据安全事件，将通报批评相关责任人。

2. 信息安全承诺书

本人已收到关于信息安全防护的相关内容。

我承诺已认真学习所提供的信息安全防护要求，并在日常工作过程中严格遵循相关防护要求，提高自身的防范意识。

我在此郑重签署本确认书，以示对以上内容的确认和承诺。如发生被上级单位认定的信息安全事件，接受公司内部通报批评。

签署人：_____

日期：_____