网站管理与应急预案

一、总则

为了更好的确保我公司网站的安全稳定运行，合理、可靠、安全、高效地组织和管理内部网站，提高内部网站的服务质量，提高维护队伍的整体素质和水平，特制定本管理制度，作为维护和管理内部网站的依据。

二、范围

本制度的适用范围包括公司官网，公司电脑系统的物理资产(包括网络设备，主机设备，安全设备等)、软件资产(操作系统，数据库，应用程序等)、数据资产(业务数据、主机数据，应用程序数据等)。

三、系统安全维护管理制度

系统维护人员应至少每天1次，对公司电脑主机设备进行检查确保各设备都能正常工作。对网站用户权限的设置应遵循最小授权和权限分割的原则，只给系统用户、数据库系统用户或其它应用系统用户授予业务所需的最小权限，应禁止为所管理主机系统无关的人员提供主机系统用户账号，并且关闭一切不需要的系统账号。

系统维护人员应制订网站系统的帐户口管理策略。对口令的选取、组成、长度、保存、修改周期做出规定。禁止使用名字、生日等易精测的字符作为口帝，也不使用单个单词或命合作为口合，组成口合的字符应包含大小写英文字母、数字、标点、控制字符等，口爷长度要求在8位以上。不应将口合存放在个人计算机文件中，或写到容易被其它人获取的地方。对于网站主机要求至少每两个月修改一次口合，若掌握口合的管理人员调离本职工作时，必须立即更改所有相关口令,严格禁止非本维护管理人员直接进入主机设备进行操作，若在特殊情况下(如系统维修、升级等)需要外部人员(主要是指厂家技术工程师、非本系统技术工程师、安全管理员等)进入公司电脑设备进行操作时，必须由系统管理员登录，并对操作全过程进行记录备案。禁止将系统用户账号及口合直接交给外部人员。

系统软件安装之后，系统维护人员应立即进行备份；在后续使用过程中，系统软件的变更以及配置的修改之前和之后，也应立即进行备份工作。

严禁随意安装、卸载系统组件和驱动程序，如确实需要，应及时评测可能由此带来的影响，并需要获得分管领导的批准。禁止在公司电脑上安装与该与网站更新服务和应用无关的其它软件。禁止在主机系统上浏览外部网站网页、接收电子邮件、编辑文档以及进行与主机系统维护无关的其它操作。禁止在主机系统上开放具有“写”权限的共享目录，如果确实必要，可临时开放，但要设置强共享口帝，并在使用完之后立刻取消共享。系统维护人员应定期进行安全漏洞扫描和病毒查杀工作，平均周一次重太发周发有后在3个工作日内进行修补；并且为了防止网络安全扫描以及病毒查杀对网络性能造成影响，应根据业务的实际情况对扫描时间做出规定应一般安排在非业务繁忙时段；当发现主机设备上存在病毒、异常开放的服务或者开放的服务存在安全漏洞时应及时上报分管领导，并取相应措施。

公司官网网站主机采用数据异地备份技术，网站主机至少保持最近三个月的系统和数据备份，以便系统的恢复。 （本公司网站采用独创阿里云异地备份技术，网站平均3天对网站内容及数据库进行异地备份，数据备份1年，最近一个月3天备份一次，最近3个月一周备份一次，最近12个月，保留月备份时间节点，采用深圳阿里云数据会同步备份到青岛阿里云，并可以在5-10分钟内回复到一年内的任何一个时间节点上）

网站应急预案

如果网站出现问题向阿里云下工单会在1小时内相应并按要求进行数据恢复或者暂时关闭网站。