北京股权交易中心认股权综合服务试点
系统安全业务规则（试行）

（2022 年 12 月制定）

第一章 总则

第一条 为规范和加强北京股权交易中心（以下称本中心）认股权综合服务试点平台信息系统（以下称服务系统）安全管理，有效防范运用服务系统进行认股权转让业务处理中产生的风险，确保服务系统安全、持续、稳定运行，制定本规则。

第二条 本规则依据《中华人民共和国信息安全风险管理规范》《中华人民共和国计算机服务系统安全保护条例》等相关文件制定，同时自动引入以下国家标准:

（一）《GB 17859-1999 计算机信息系统安全保护等级划分准则》;

（二）《GA/T 390-2002 计算机信息系统安全等级保护通用技术要求》;

（三）《GA/T 387-2002 计算机信息系统安全等级保护网络技术要求》;

（四）《GA/T 388-2002 计算机信息系统安全等级保护操作系统技术要求》;

（五）《GA/T 389-2002 计算机信息系统安全等级保护数据库管理系统技术要求》。

第二章 信息安全管理内容

第三条 信息安全需求分析具体如下:

（一）物理安全：从外界环境、基础设施、运行硬件、介质等方面为服务系统安全运行提供基本的底层支持和保障。安全需求主要包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷电、防火、防静电;

（二）系统安全：提供安全的操作系统和安全的数据库管理系统，以实现操作系统和数据库管理系统的安全运行。安全需求包括：操作系统、数据库系统、服务器安全需求、基于主机的入侵检测、基于主机的漏洞扫描、基于主机的恶意代码的检测与防范、基于主机的文件完整性检验、容灾、备份与恢复;

（三）网络安全：为服务系统能够在安全的网络环境中运行提供支持。安全需求包括：信息传输安全需求、网络边界防护安全需求、网络上的检测与响应安全需求;

（四）数据安全：实现数据的机密性、完整性、可控性、不可否认性，并进行数据备份和恢复;

（五）应用安全：保障服务系统的各种业务的应用程序安全运行，其安全需求主要涉及口令机制和关键服务系统的对外接口。

第四条 服务系统安全管理对象具体如下:

（一）网络及相关硬件设备，如服务器、存储设备、业务专用机等;

（二）操作系统，指运行在服务器、办公用机、业务专用机之上的电脑操作系统;

（三）应用系统，指运行在操作系统之上的专用服务系统、数据库系统、电子邮件、浏览器等。

第三章 信息安全管理机构及职能

第五条 服务系统安全管理由信息技术部负责。

第六条 服务系统安全管理具体工作内容如下:

（一）制定服务系统的安全管理制度和措施;

（二）制定服务系统的安全应急计划;

（三）建设和运行管理服务系统安全防护系统;

（四）服务系统安全审查;

（五）服务系统数据的安全管理;

（六）组织服务系统安全应急演练;

（七）服务系统安全事故的处理和调查。

第七条 服务系统使用部门应当按照相关规定和操作手册正确操作和使用系统，并负责对本部门人员进行安全教育和管理。

第四章 用户、口令及权限管理指引

第八条 权限分离原则具体如下:

（一）网络设备、域、操作系统、数据库系统中的用户和口令由信息技术部统一管理;

（二）各应用系统中的用户和口令由相关业务部门各自管理;

（三）关键服务系统的管理员用户与相应操作系统的管理员用户、相应数据库系统的管理员用户应当分别由不同人员掌管。

第九条 权限分配最小化原则：总是分配给最少的人员以最小的权限。

第十条 权限使用最小化原则：总是选择权限最小的用户来完成工作，尽量减少使用管理员权限的次数。

第十一条 权限明确原则：建立用户应当遵循明确责任原则，做到专人专户和专户专用。

第十二条 定期检查原则：应当每年审核用户权限设置情况，发现设置不合理或者冗余用户时，应当立即进行纠正。

第十三条 用户口令的设置原则具体如下:

（一）普通用户口令长度不得小于8位同时应当包含数字、字母及特殊字符，且不容易被破解。用户口令建议定期更换，且2个更改周期内不重复使用;

(二)服务系统相关的管理员用户口令长度不低于8位，并采用数字、字母、特殊字符混排的方式。口令要求每三个月更改一次，且2个更改周期内不重复使用，同时保留更改记录。

第十四条 口令的存放原则：不要将密码以明文的形式储存或者记录在任何能够被任何非授权人员访问的地方。

第十五条 用户及口令的保密原则具体如下:

（一）工作人员口令由其本人掌握，严禁泄露。如发现

或怀疑口令泄露，应当及时更换;

（二）严禁盗用他人账号;

（三）严禁与他人共享账号。如果发现自己的账号被他人非法使用，应当及时制止并向信息技术部报告。

第十六条 权限定期检查原则：信息技术部应当定期检查权限的可用性及正确性。

第十七条 对管理员的限制：对管理员用户的使用应当进行有效的限制，包括设置网段号、限制登录站点和设置错误登录尝试次数等。

第十八条 服务系统业务人员离职后，相关部门负责人应当及时通过邮件或 OA 内部协同通知信息技术部。信息技术部在收到通知后应当及时撤销或者修改离职人员所使用的用户名、密码及相关权限，并应当保留好日志备查。

第五章 网络安全指引

第十九条 网络设备安全要求如下:

（一）所有网络设备的安装、调试、配置由信息技术部统一负责;

（二）所有网络设备应当由信息技术部指定人员设置管理员密码，密码长度至少为 8 位，密码应当由字母、数字和特殊字符混排;

（三）网络设备的访问口令不能使用缺省口令。管理员密码应当定期修改，2 个月至少修改一次;

（四）无线网络交换或者路由设备应当设置适当的认证

规则以限制匿名接入;

（五）所有网络设备应当定期巡检;

（六）各类网络设备未经信息技术部的允许不可带出所在地的机房;

（七）所有网络配置、系统配置只能在闭市后调整;

（八）无用信息节点应当与网络交换机端口断开;

（九）应当关闭交换机闲置端口设置。

第二十条 网络线路安全要求如下:

（一）通讯线路的开通由信息技术部负责实施;

（二）骨干线路应当选择不同电信运营商的通讯线路，组成互为备份的双线骨干线路;

（三）不得把网络设备和网络线路暴露在非授权人员能够接触到的地方。

第二十一条 IP 地址规范如下:

（一）所有设备的 IP 地址由信息技术部统一规划，任何人不得随意变更;

（二）任何人不可盗用 IP 地址。

第二十二条 远程访问的安全要求如下:

（一）远程访问方式统一由信息技术部规划并实施;

（二）远程访问所使用的用户名和密码由信息技术部统一管理;

（三）建立远程访问权限的开通由相应部门提出申请，信息技术部统一办理，不得私自随便设立;

（四）访问用户的密码不得少于12位，并不得采用简单的密码。

第六章 操作系统安全指引

第二十三条 物理安全

不同功能的服务器应当做到物理隔离或逻辑隔离，按功能不同存放在不同的网络中。

第二十四条 日志及审核管理具体如下:

（一）根据系统需要，服务器、业务专用机应当启用相应的日志记录。日志记录应当包括：登录，登出，系统报警，安全日志，重要应用程序日志，重要文件访问日志。为保证日志的准确性，应当正确设置计算机时钟。对服务器应当启用操作系统中的审计功能;

（二）服务器和业务专用机的操作系统管理员应当每周检查系统日志，对发现的问题及时纠正，并做好记录;

（三）服务器和业务专用机的操作系统管理员应当定期对日志进行归档。

第二十五条 系统补丁及升级管理具体要求如下:

（一）操作系统管理员应当及时安装新发布的操作系统补丁。对于关键的服务器，安装补丁前应当在备用的服务器上进行补丁的测试，测试通过后方可在生产服务器上安装。安装补丁前应当做好系统备份，以防安装补丁后出现问题。如果补丁安装不成功或导致系统工作不正常，应当卸载补丁，恢复原状态;

（二）办公用机的管理员应当使用 Windows 自动更新的功能，及时地从网络上升级操作系统。

第二十六条 防病毒服务器、业务专用机及办公用机应当安装由信息技术部指定的网络防毒软件，日常更新病毒库。

第二十七条 服务器的无人值守要求如下:

（一）服务器应当设置自动屏幕保护程序，并启用离开后自动锁定功能，同时要求用户在离开时将屏幕锁住;

（二）登录到系统时，完成任务后或长时间不使用时应当从系统注销登录。

第二十八条 服务器的版本管理和应用软件管理

服务器的操作系统和应用软件的版本由信息技术部统一控制，操作系统和应用软件的安装介质由信息技术部统一控制。

第二十九条 未经信息技术部许可，任何人不得运行各种漏洞扫描软件、抓包嗅探软件、IDS 软件等安全工具。

第七章 数据及数据库管理系统安全指引

第三十条 日志及审核管理要求如下:

（一）针对系统需要，启用相应的日志记录，日志记录应当包括：登录，登出，系统报警，安全审核日志。为保证日志的准确性，应当正确设置计算机时钟;

（二）服务系统的日志应当集中管理和备份，备份时间不得少于 1 年;

（三）数据库管理员应当做好数据库事务日志的备份和

归档工作，不得随意篡改、销毁、删除事务日志的备份;

（四）数据库系统管理员应当定期检查系统日志，对发现的问题及时纠正，并做好记录。

第三十一条 补丁及升级要求如下:

（一）数据库系统管理员应当及时安装新发布的数据库系统补丁;

（二）对于服务系统，安装补丁前应当在备用的服务器上进行补丁的测试，测试通过后方可在生产服务器上安装;

（三）安装补丁前应当做好备份，以防安装补丁后出现问题。如果补丁安装不成功或导致系统工作不正常，应当卸载补丁，恢复原状态。

第三十二条 数据安全管理要求如下:

（一）应当做好服务系统业务数据的管理工作，防止数据丢失、泄密和被篡改;

（二）应当注意保护测试数据中可能包含的敏感内容。在将真实的数据用作测试之前，应当先将保密信息删除。

第八章 服务系统安全指引

第三十三条 物理安全具体要求如下:

（一）服务系统所在服务器应当设置严格的访问控制，与该系统不相关的网络、服务器及办公用机应当与之进行有效的隔离;

（二）服务系统所在服务器应当符合操作系统安全的相关规定。

第三十四条 日志及审核要求如下:

（一）在不影响服务器性能的情况下，尽可能地启用服务系统所有的审核和日志功能;

（二）服务系统所在服务器应当符合操作系统及应用安全的相关规定。

第九章 外来设备、数据及人员访问管理安全指引

第三十五条 外来设备接入服务系统网络之前应当联系信息技术部确认其没有携带病毒、木马或其他恶意程序，以及没有运行妨碍服务系统网络的软件和程序，如 DHCP 服务器、网络扫描程序等。

第三十六条 外来数据的管理具体要求如下:

（一）外来的软件及数据在使用之前应当经过杀毒处理;

（二）不得随便下载和使用不安全网络上面提供的任何软件和数据;

（三）不经相关部门批准，外来业务人员不得访问服务系统任何关键数据。如确因业务需要，需经过相关业务部门和信息技术部的领导共同签字批准，并由相关业务部门的人员全程陪同录像下进行操作。

第三十七条 外来人员操作系统的管理要求如下:

外来业务人员需要操作本中心系统或者需要进入机房时，应当经部门分管领导及信息技术部分管领导签字批准后，由机房值班人员陪同进行，不得随意操作和触动与其工作无关的设备，不得进行工作之外的其他活动。

第十章 服务系统安全的应急管理

第三十八条 安全事件的定义

安全事件，就是干扰或打断系统的正常运行，使其陷入某种级别危机的事件，比如黑客入侵、拒绝服务攻击、未经授权的网络通信和系统操作等。

第三十九条 成立信息安全应急指挥小组

应当成立信息安全应急指挥小组，对安全紧急事件的处理进行统一指挥。组长应当由信息技术部分管领导担任。

第四十条 信息安全事件的报告

当发现非不可抗力、非设备故障等原因引起网络瘫痪、业务中断、系统宕机等突发事件时，应当立即通知信息技术部。

第四十一条 信息安全事件的应急处理

当安全事件发生后，相关人员应当根据事先制定的安全故障、事故或灾难的级别和安全事件的性质采取相应的应急措施对安全事件进行应急处理，处理的原则主要包括:

（一）遵照放小保大原则，保证主要业务正常运行，尽快恢复全部系统或网络的正常运转;

（二）故障设备为业务设备时，应当参照相关应急预案执行；故障设备为办公设备时，应当立即将故障设备断网隔离，但不要立即对办公用机进行处理，应当先保护现场，以便事后检查原因;

（三）使系统和网络操作所遭受的破坏最小化;

（四）检索并清除病毒及黑客留下的后门和木马客户端

等。

第四十二条 信息安全事件分析与问责要求如下:

（一）信息技术部应当建立安全应急事件库，并对安全事件进行分析和总结;

（二）信息安全应急事件库，包括各种发生过的或很可能发生的具体安全事件，以及每种安全事件的最佳应急措施和备用方案，以便为后面的应急恢复工作做好知识储备。另外，库中还应当包括发生过的安全事件的应急响应详细记录;

（三）安全事件分析，是指针对记录内容中攻击事件的来源、攻击来源反跟踪、攻击的原因、攻击产生的影响和后果，以及攻击所采用的技术手段等进行分析和归类录入应急事件库中;

（四）经分析如发现是由于没有按照信息技术部发布的规范进行使用或操作的行为所引发安全事件或导致事件等级升高的，则对当事人进行问责；如发现信息技术部发布的规范存在缺陷的，则及时修补规范。

第十一章 附则

第四十三条 本规则由本中心负责解释和修订。

第四十四条 本规则自发布之日起施行。