用户上机承诺书

1. 引言

上海超级计算中心（SSC）（以下简称中心）的计算设备，包括硬件、软件、网络和存储设备，是一个重要的有限资源。因此，用户有义务保护中心设备并确保设备被合理的使用。此外，用户也要遵守法律和其他义务，保护其他使用中心资源的用户正常使用以及这些用户的知识产权不被侵犯。

您的合作，将会使中心的设备及资源发挥最大效用。您的协助也可确保您可以正常用机，同时也是对其他用户正常用机的最大帮助。

本须知是用户使用中心设备时必须要阅知和遵守的规范。因此请您详细阅读本须知的所有内容，当您签署承诺书后即被视为您已阅读并同意接受本文所有条款的规定。对于不正确的使用设备的情况会导致相应惩罚。

如果您在签署前对本须知有任何疑问，请及时和项目经理联系。

2. 要求

2.1 账户管理

您的账户要在被授权的情况下正确使用。

2.1.1 非共享账户

一个账户只提供给唯一用户使用。不可以和其他用户共享。用户认证也不能分享。对于一个用户但有多个上机人员的情况，请仔细斟酌、确定。超算中心视用户正式提供的上机人员名单均为合法用户。

2.1.2 口令的保护

口令和认证是账户访问的关键。您要确保口令和认证安全。更多的信息请参阅第 5 章指南部分。

2.1.3 授权/满足要求的使用

2.1.3.1 授权使用

您的行为仅限您的申请书上声明并被批准的行为。账户的使用应当被限制在那些行为之内。

2.1.3.2 不可接受行为

下列行为是不准许的且可能导致第 3 节中述及的惩罚：

- 在未授权的情况下，使用您申请且被批准使用资源以外的其他资源，以及申请且被批准的行为外的其他行为；
- 可能损害或妨碍设备正常运转的行为，即使您在此前并不知晓该行为会导致的后果。因此用户有必要熟练掌握有关使用技术、密切地和中心技术人员沟通、不执行无把握、不确定后果的操作；
- 试图或通过非正常手段阅读、改变、分发或者拷贝其他用户的数据或软件；
- 在未授权的情况下，通过使用中心资源以试图得到与中心相连的网络上其他计算中心资源的访问行为；
- 违反国家及地方法律法规的行为

2.1.4 报告可疑行为

如果您的账户上的发现可疑行为，请您尽快报告项目经理。

2.2 数据机密性及完整性

您要确保任何知识产权的机密性或是其他在中心资源上使用的数据的安全。

请同项目经理协商共同确定资料、数据及项目的密级，以及备份方案,防止意外造成数据丢失

2.3 软件许可

中心确保提供给您使用的所有软件系统均有合法授权。同样，您在中心计算机系统上安装和使用的软件要求必须有合法授权。请不要在您的目录下安装和使用可能引起知识产权纠纷的软件。用户不应当复制拥有版权的软件或材料，除非经拥有者或版权所有者允许。如有发生，您将承担相应的法律责任，与中心无关。

2.4 网络要求

不利用中心的网络系统和网络服务从事以下活动：

- 未经允许，进入中心信息网络或者使用中心计算机信息网络资源的；
- 未经允许，对计算机信息网络功能进行删除、修改或者增加的；
- 未经允许，对进入计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；
- 故意制作、传播计算机病毒等破坏性程序的；
- 其他危害计算机信息网络安全的行为。

不以任何方式干扰中心的网络服务。中心将保留追究其法律责任的权利并有权将其提交给相关部门处理，具体请参阅第 3 节。

2.5 作业管理

您的计算作业必须通过指定的作业管理系统提交至指定的队列中，您能同时使用的最大计算资源由中心审批后确定。您应密切保持对您所提交的作业的排队和运行状况、磁盘空间等的监控。

出现任何异常请首先查找以下原因：您的账户是否仍然有效；是否未通过指定作业管理系统提交；是否未提交至指定队列；授权磁盘是否已满；队列状态是否忙等。其他原因请及时和您的项目经理保持联系。

2.6 上机总结报告

用户在一个项目结束或结束上机时应提交上机总结报告，参见《用户上机流程管理规定》，本报告对该用户再次使用资源的申请批准具有相当的参考作用。

2.7 机房管理

用户本地上机应在中心指定区域，未经允许不得进入主机房、网络机房。用户进入用户工作室要遵守相关规定，参见《用户工作室管理规定》。

2.8 消防要求

用户进入中心所属区域必须遵守《消防安全规定》。不允许在中心任何范围内吸烟，除笔记本电脑外，不得在中心将任何电气设备接入。

2.9 其他要求

2.9.1 特殊用户要求

特殊用户要了解并遵守国家或地方法律法规或者其组织机构所要求遵守的超过本承诺书的其他特殊要求。

2.9.2 对非学术用户要求

非学术用户（公司的、产业的机构，政府机关等）常常要比其他用户有更迫切的使用要求，中心在资源紧张时会采取一定的措施确保他们的需求。

2.9.3 致谢

任何使用本中心资源和由中心提供技术支持完成的出版物（论文、书籍、网页、宣传资料等）必须对中心进行注明并致谢。

3. 处罚措施

不履行遵守这份协议书可能同时导致多种强制性处罚。

3.1 账户暂停使用/撤消

如果您执行危险操作或非法滥用中心资源，您的账户会被临时暂停直至永久取消上机资格。账户如果被怀疑执行危及自身账户、系统安全的操作或者是带恶意的或非法的行为，则会在不被提前通告的情况下被暂停使用。若有上述情况发生且您并不明原因，请及时和项目经理联系。如果帐号使用到期，在项目经理已通知您的情况下，十个工作日内未办理继续使用主机的申请，中心有权将帐号删除。

若用户的行为不符合用户申请里提到的服务条款，中心将有权做出独立判断并立即取消用户服务账号。

3.2 资源权限取消

本处罚可导致您当前资源权限被部分或全部取消，且未来可能不能再次获得。

3.3 行政诉讼

违反上机规定的行为会被报告给您的主管机构。

3.4 民事处罚

民事赔偿可被作为追究资源在未被授权情况下使用所带来的补偿代价或是由于不良行为所导致的事件的补偿费用。

3.5 刑事处罚

用户需对自己在中心网络资源上的行为承担法律责任。用户在中心网络违反国家法律、法规或相关政策，中心的系统记录会被作为用户违反法律的证据。

3.6 其他赔偿

如发生损害中心机器设备或是引发其他严重事故，造成中心或其他用户软硬件及其他损失，对于事故负责方，中心有权保留和送交监测材料给相关部门以用于对其进行调查和诉讼。

4 声明

4.1 附加要求

像在§2.9 里声明的一样，特殊用户可能要受到超过这份文件所规定的要求的影响。

4.2 支持/诊断访问

中心技术人员经授权，可以回访文件以用于帮助一个特定用户或者为中心计算机系统提供诊断调查。

4.3 监测

在政策规定和法律的允许下，用户行为会被监测用于保护数据和资源。

4.4 访问通知

在没有被明确授权或提前通知的情况下，对用户的数据和通讯信息的访问通常将不能被执行。紧急的情形下，访问后会提供事后通知。

5. 指南

下面所列的是可以帮助维持您的账户安全的一些建议。

5.1 口令管理

- 不要将您的口令写在任何可以轻易找到的地方。
- 不要把您的口令告诉任何人，甚至是中心的技术支持人员。如有人坚持需要您的口令，请报告给您的项目经理。
- 不要将您的口令保存在未加密的文件里，或通过邮件、Email 传送口令。
- 挑选难猜的口令。
- 定时修改您的口令。

5.2 应对可疑行为

适当的联系方法请参阅后面的第 6 部分

5.2.1 口令暴露

如果您认为您的口令已被他人获知，请立即修改您的口令。

5.2.2 危害到账户安全的或可疑的行为

如果您认为您的账户安全被侵犯或发现有可疑行为的迹象，包括：

- 在您的主目录或是工程领域里的发现不是您创建的文件
- 文件的变更或是删除不是由您自己操作的
- 您的资源分配，同您认为您已经使用的之间有差异

请执行下列操作：

- 立即通知您的项目经理
- 不要修改在您的账户里发现的可疑文件
- 不要执行您发现的未知程序
- 如果可能，不要使用您的账户直到问题被解决

6. 联系方式

6.1 一般帮助

关于本承诺书的一般问题，请联系项目经理或技术人员。

6.2 可疑行为

如发现涉及侵犯账户或系统安全的可疑行为，请及时通报给项目经理。

6.3 口令和认证的修改

主机账号不可更改，为您在申请时确定的唯一账号。防火墙口令不能自行更改，可联系项目经理进行修改。曙光 4000A 的口令可自行修改，要求在 LSF 的登录 web 上修改，不能在命令行中直接使用 yypasswd 命令。

7. 承诺声明

签署用户上机承诺书即表明了所有被授权用户上机使用人员已阅知本承诺书且理解了其中信息，同时确认遵守承诺书里声明的规定和程序。

上海超级计算中心会在必要时修改承诺书的条款，条款一旦发生变动，中心将会通告所有的用户。如果您不接受新的条款，请及时告之项目经理。否则，将默认您同意新的承诺书。