附件

工业和信息化领域数据安全风险信息报送与共享工作指引（试行）

第一章　总则

第一条 为加强工业和信息化领域数据安全风险信息获取、分析、研判和预警工作，及时掌握工业和信息化领域数据安全整体态势，提高数据安全风险处置能力，根据《中华人民共和国数据安全法》等法律法规，制定本指引。

第二条 本指引所称数据安全风险信息，是指通过检测、评估、信息搜集、授权监测等手段获取的，包括但不限于数据泄露、数据篡改、数据滥用、违规传输、非法访问、流量异常等数据安全风险:

（一）数据泄露，包括但不限于数据被恶意获取，或者转移、发布至不安全环境等相关风险;

（二）数据篡改，包括但不限于造成数据破坏的修改、增加、删除等相关风险;

（三）数据滥用，包括但不限于数据超范围、超用途、超时间使用等相关风险;

（四）违规传输，包括但不限于数据未按照有关规定擅自进行传输等相关风险;

（五）非法访问，包括但不限于数据遭未授权访问等相关风险;

（六）流量异常，包括但不限于数据流量规模异常、流量内容异常等相关风险;

（七）其他信息，包括由相关政府部门组织授权监测的暴露在互联网上的数据库、大数据平台等数据资产信息，以及有关单位掌握的威胁数据安全的其他风险信息等。

第三条 本指引所称风险信息报送，是指有关单位向工业和信息化部、地方工业和信息化主管部门、地方通信管理局报送数据安全风险信息的行为。

第四条 本指引所称风险信息共享，是指经工业和信息化部、地方工业和信息化主管部门、地方通信管理局审核、授权后，向有关部门、单位告知风险提示的行为。

第五条 风险信息报送与共享工作坚持“及时、客观、准确、真实、完整”的原则，不得迟报、瞒报、谎报。

第二章　组织机构及职责

第六条 工业和信息化部指导、监督工业和信息化领域数据安全风险信息报送与共享工作。具体工作由工业和信息化部网络安全管理局（以下简称网安局）会同各相关业务司局共同开展。其中，网安局统筹协调风险信息报送与共享工作，各相关业务司局负责参与风险信息评估、研判、处置等工作。

第七条 地方工业和信息化主管部门负责本地区工业领域

数据安全风险信息报送与共享工作。

地方通信管理局负责本地区电信和互联网领域数据安全风险信息报送与共享工作。

第八条 工业和信息化部（网安局）组织建设、运行工业和信息化领域数据安全风险信息报送与共享平台（以下简称平台），收集、汇总数据安全风险信息，并发布、通报风险提示。

第九条 工业和信息化部选择有条件的部属单位作为支撑单位，负责运行维护平台，并支撑工业和信息化部（网安局）开展风险信息报送与共享工作。

第三章　风险信息报送

第十条 工业和信息化部（网安局）鼓励部系统各单位、安全企业、数据处理者、科研院所、行业组织等单位（以下简称风险报送单位）开展风险信息报送，遴选支撑服务能力强、技术水平高、报送信息质量优的单位建立风险直报单位名录，并实施名录动态管理。

地方工业和信息化主管部门、地方通信管理局应当组织开展本地区风险报送单位遴选、推荐等工作，建立本地区风险报送单位名录，并加强名录管理。

第十一条 风险直报单位应当通过平台直接向工业和信息化部（网安局）报送数据安全风险信息。

其他风险报送单位应当通过平台及时向所在地工业和信息化主管部门、通信管理局报送掌握的工业、电信和互联网领域

数据安全风险信息。

第十二条 地方工业和信息化主管部门、地方通信管理局应当组织开展本地区风险信息报送工作，审核研判本地区收到的风险信息，及时向工业和信息化部（网安局）报送涉及重要数据和核心数据的、跨地区的或者可能造成重大事件的相关风险信息，并每半年向工业和信息化部（网安局）报送风险信息报送工作总结。

第四章　风险信息研判与共享

第十三条 工业和信息化部（网安局）组织支撑单位对部级平台收到的风险信息进行评估和研判，对于确认的风险信息开展共享和通报，达到应急标准的，应当同时启动应急预案。

支撑单位对风险信息进行分类、研判、整理，及时分析总结风险信息报送与共享情况，并向工业和信息化部（网安局）报送。

第十四条 工业和信息化部（网安局）根据数据安全风险影响范围等情况，分别开展以下风险信息共享和通报工作:

（一）对于可能影响社会公众的风险信息，可通过部网站等渠道通报;

（二）对于区域性的风险信息，通报至有关地方工业和信息化主管部门或者地方通信管理局;

（三）对于能够确定具体通报单位的，同时向该单位主体及其所在地工业和信息化主管部门或者通信管理局通报;

（四）工业和信息化部（网安局）加强数据安全态势分析，不定期通报行业数据安全情况。

第十五条 地方工业和信息化主管部门、地方通信管理局应当及时接收工业和信息化部（网安局）发送的数据安全风险信息，并指导、督促相关单位开展风险处置。应当及时研判分析本地区数据安全风险信息，并将相关信息通报至相关单位进行处置。

第十六条 数据处理者接到通报信息后，应当及时处置风险，并按要求反馈处置情况。

第五章　保障措施

第十七条 工业和信息化部（网安局）组建数据安全风险分析专家组，为风险信息报送与共享工作提供技术咨询和决策支持。

第十八条 工业和信息化部（网安局）每年对风险报送单位报送信息的数量、质量等进行评比，对表现突出的单位予以鼓励。

第十九条 地方工业和信息化主管部门、地方通信管理局、风险报送单位应当指定风险信息报送与共享工作联络员，报工业和信息化部（网安局）备案。联络员和联络方式发生变化时，应当在5个工作日内报送变更情况。应当加强数据安全风险信息报送与共享工作保障，对表现突出的风险报送单位予以鼓励。

第二十条 参与风险信息报送与共享工作的相关机构和人

员应当对获悉的信息承担保密义务，不得泄露或者非法向他人提供。

第二十一条 地方工业和信息化主管部门、地方通信管理局应当参照本指引，建立完善本地区工业、电信和互联网领域数据安全风险信息报送和共享工作机制。

第二十二条 本指引自发布之日起实施。

附件 1：风险信息报送模板

数据安全风险信息

xx 年 xx 月 xx 日，xx（风险报送单位）发现 xx 公司（风险所在单位）xx 系统存在数据安全风险。有关情况如下。

一、风险基本情况

（一）风险类别和级别

风险类别[1]:

风险级别[2]:

（二）风险涉及数据情况

涉及数据类型[3]:

涉及数据级别[4]:

涉及数据量:（暂时无法确定的可写暂不确定）

（三）风险产生时间

xx 年 xx 月 xx 日（暂时无法确定的可写暂不确定）

（四）风险范围

影响地区:

影响单位:

影响行业:

---

[1] 参考本指引第二条所列举的风险类型。

[2] 风险级别分为高危、中危、低危。其中，高危风险主要指涉及重要数据或核心数据的，或者涉及数据量大、影响区域范围广的风险，中危风险主要指涉及数据量较少、影响范围较小的风险，低危风险主要指造成轻微影响的风险。

[3] 数据类型参考《工业和信息化领域数据安全管理办法（试行）》中列举的主要类型，可在此基础上进行细分类。

[4] 数据级别包括核心数据、重要数据、一般数据。

（五）风险概述

简要概述风险情况

（五）其他风险相关信息

系统名称:

系统域名:

IP 地 址:

端　　口:

风险 URL:

IP 所属地区:

IP 所属运营商:

ICP 备案号:

二、风险分析

描述风险产生原因、发现方式、验证情况及风险后果影响，并提供截图等证明。

三、风险处置建议

针对风险提出处置建议。

四、风险报送单位

单位名称:

联系人及联系方式:

附件 2：风险信息报送工作总结模板

数据安全风险信息报送工作总结

xx 年 xx 月至 xx 月，xx（主管部门）数据安全风险信息报送工作总结如下。

一、风险报送基本情况

（一）风险类型与级别情况

报送的风险包括数据泄露 xx 起，数据篡改 xx 起，数据滥用 xx 起，.....。其中，高危风险 xx 起，中危风险 xx 起，低危风险 xx 起。

（二）风险地域分布情况

报送的风险涉及 xx 等共 xx 个城市，风险数量最多的前三位城市分别是 xx（xx 起）、xx（xx 起）、xx（xx 起）。高危风险最多的前三位城市分别是 xx（xx 起）、xx（xx 起）、xx（xx 起）。

其中，跨地区的风险有 xx 起，主要涉及 xx 等地区。

（三）风险行业分布情况

报送的风险涉及 xx 等共 xx 个行业，风险数量最多的前三位行业分别是 xx（xx 起）、xx（xx 起）、xx（xx 起）。高危风险最多的前三位行业分别是 xx（xx 起）、xx（xx 起）、xx（xx 起）。

（四）风险涉及数据情况

报送的风险涉及 xx 等数据类型。其中，涉及 xx 类的有 xx

起，……，涉及 xx 类的有 xx 起；涉及核心数据的有 xx 起，涉及重要数据的有 xx 起，涉及一般数据的有 xx 起。已研判确定存在风险的数据量是 xx。

（五）风险通报处置情况

已通报 xx 家企业进行风险处置，xx 家已完成处置。

二、存在的问题

三、下一步工作计划及建议

附件：风险报送与处置情况汇总表

序号	风险报送时间	风险名称	风险类别与级别	风险所在单位	风险处置情况	风险报送单位

附件 3

工业和信息化领域数据安全风险报送单位申报要求

申报工业和信息化领域数据安全风险报送单位，应当符合下列基本条件:

一、在中华人民共和国境内注册成立，取得独立法人资格;

二、遵守中华人民共和国法律法规和相关规定，在信用中国的查询信息中无不良记录，5 年内无违法违规记录，对国家安全、社会秩序、公共利益不构成威胁;

三、注册资金在 500 万元人民币以上，组织管理结构和产权关系明晰，独立经营核算;

四、从事数据安全相关工作 3 年以上，在工业、电信和互联网数据安全领域有一定的综合实力和技术优势，有固定的场所和必要的设施，具备必要的数据安全风险发现、分析、研判、处置等技术能力和业务积累;

五、具有 2 年以上数据安全相关工作经历的技术团队人员不少于 20 人，其中取得数据安全、网络安全、计算机等相关专业资质证书的人员不少于 10 人，相关人员 5 年内无违法违规记录;

六、支持提供 7×24 小时风险研判、应急处置等相关服务;

七、自愿签订承诺书，严格遵守相关要求。自觉接受工业和信息化部（网络安全管理局）监督和指导。发生违法违规行

为或违约行为的，将自动撤销风险报送单位资格，5 年内不得重新申请。

附件 4

工业和信息化领域数据安全风险报送单位承诺书

工业和信息化部网络安全管理局:

我单位申报工业和信息化领域数据安全风险报送单位，严格遵守相关工作要求，并自愿作出以下承诺:

一、不以非法方式开展数据安全风险监测、检测等工作;

二、不以非法方式收集数据安全相关风险信息;

三、及时报送所发现的数据安全风险，未经主管部门确认，不擅自披露风险;

四、对报送信息的客观性、准确性、真实性、完整性负责;

五、对报送信息内容负有保密责任，所报送的信息内容不涉及国家秘密、个人隐私信息和其他敏感信息;

六、支持提供 7×24 小时风险研判、应急处置等相关服务;

七、存在责任落实不到位、造成重大安全事件、严重违法违规等行为的，将妥善处理善后事宜。

我单位对违反上述承诺导致的后果承担全部法律责任。

单位负责人:

（加盖公章）

xx 年 xx 月 xx 日