广东省工业和信息化领域企业信息安全事件应急预案

（试行）

1 总则

1.1 编制目的

加强广东省工业和信息化领域企业信息安全（以下简称企业信息安全）应急工作管理，建立健全企业信息安全应急工作机制，提高应对企业信息安全事件的组织协调和应急处置能力，确保及时有效地控制、减轻和消除企业信息安全事件造成的危害和损失，保障工业生产稳定运行，维护经济安全和人民生命财产安全。

1.2 编制依据

《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《国家网络安全事件应急预案》《工业控制系统信息安全事件应急管理工作指南》《工业和信息化领域数据安全管理办法（试行）》《工业和信息化领域数据安全事件应急预案（试行）》《工业互联网安全分类分级管理办法》等法规政策和《信息安全技术 网络安全事件分类分级指南》（GB/T 20986-2023）《信息安全技术 工业控制系统信息安全分级规范》（GB/T 36324-2018）等标准规范。

1.3 适用范围

在广东省辖区内发生的工业和信息化领域企业信息安全事件应急处置活动，应当遵守相关法律法规和本预案的要求。工业和信息化部、广东省工业和信息化厅等相关主管部门对重大活动期间企业信息安全事件应急处置工作另有规定的，从其规定。

1.4 事件定义

本预案所称工业和信息化领域企业信息安全事件，是指由于人为原因、软硬件缺陷或故障等，对工业和信息化领域企业数据安全、工业互联网安全、工业控制系统（以下简称工控系统）信息安全等造成危害，导致或可能导致企业网络和信息系统、工控系统或者其中的工业数据遭篡改、破坏、泄露或者非法获取、非法利用，影响正常工业生产，对国家安全、公共利益或者个人、组织合法权益造成危害的事件。

1.5 事件分级

根据工业和信息化领域企业信息安全事件对国家安全、企业网络和信息系统、生产运营、经济运行等造成的影响范围和危害程度，将企业信息安全事件分为五级：特别重大企业信息安全事件、重大企业信息安全事件、较大企业信息安全事件、次级企业信息安全事件、一般企业信息安全事件（见附件 1）。

1.6 工作原则

统筹发展和安全，坚持政府指导、企业主体，遵循“谁管业务、谁管信息安全”原则，落实工业和信息化领域企业信息安全主体责任。坚持密切协同、分级负责，实现企业信

息安全突发事件应急处置的科学化、程序化与规范化。坚持居安思危、预防为主，充分发挥各方力量，共筑企业信息安全保障体系。

2 组织机构与职责

2.1 省工业和信息化厅

省工业和信息化厅按照工业和信息化部、省委省政府相关工作要求，在省数据安全工作协调机制和省委网信办的统筹下，协同开展工业和信息化领域企业信息安全应急管理工作，建立与同级网信、公安、通信管理等相关部门的应急联动工作机制，按照有关法律、行政法规，依法配合有关部门开展企业信息安全事件应急处置工作。

2.2 地市工业和信息化主管部门

各地市工业和信息化主管部门在同级数据安全工作协调机制和网信部门的统筹下，协同开展本地区工业和信息化领域企业信息安全事件应急处置工作，结合实际制定本地区工业和信息化领域企业信息安全事件应急预案，推动工业和信息化领域企业落实主体责任，指导企业建立健全信息安全管理制度。

2.3 工业和信息化领域企业信息安全应急专家队伍

省工业和信息化厅积极吸收引进信息安全领域和行业领域专家，组建工业和信息化领域企业信息安全应急专家队伍，围绕企业信息安全态势研判、决策咨询、宣贯培训、科技支撑、技术研究等方面提供智力支撑，协助各地市工业和信息化主管部门开展企业信息安全应急处置工作。

2.4 工业和信息化领域企业信息安全应急支撑机构

省工业和信息化厅、各地市工业和信息化主管部门根据需要遴选工业和信息化领域企业信息安全应急支撑机构，负责开展企业信息安全事件预防保护、监测预警、应急处置、攻击溯源等工作，为工业和信息化领域企业信息安全应急处置提供技术支撑。

2.5 工业和信息化领域企业

各工业和信息化领域企业应严格落实信息安全主体责任，负责本单位信息安全事件预防、监测、应急处置、报告等工作，应当根据应对信息安全事件的需要，制定本单位信息安全事件应急预案。

3 监测与预警

3.1 预警监测和报告

省工业和信息化厅依托工业和信息化领域企业信息安全应急支撑机构、有关平台等，对全省工业和信息化领域企业的网络和信息系统、工控系统、相关数字化产品及解决方案等开展安全监测，在可控范围内共享企业信息安全相关威胁情报信息。其中经研判认为可能发生重大及以上企业信息安全事件的，应当立即向工业和信息化部、省委省政府报告，同时通报同级数据安全工作协调机制、网信、公安等部门。

各地市工业和信息化主管部门应密切监测本地区企业信息安全情况，并定期将重要监测信息报省工业和信息化厅。其中经研判认为可能发生较大及以上企业信息安全事件

的，应当立即向省工业和信息化厅、市委市政府报告，同时通报同级数据安全工作协调机制、网信、公安部门。

各工业和信息化领域企业组织开展本单位信息安全监测工作，可定期将重要监测信息报属地工业和信息化主管部门。其中经研判认为可能发生次级及以上企业信息安全事件的，应当立即向属地市级工业和信息化主管部门报告（模板见附件2）。

3.2 预警分级

工业和信息化领域企业信息安全事件预警等级分为五级：由高到低依次用红色、橙色、黄色、紫色、蓝色表示，分别对应发生或可能发生特别重大、重大、较大、次级及一般信息安全事件。

各级工业和信息化主管部门及时汇总分析企业信息安全风险和预警信息，必要时组织企业信息安全应急支撑机构、专家、相关企业进行会商谈判，明确预警等级。

3.3 预警发布

省工业和信息化厅根据工业和信息化领域企业信息安全监测情况，发现可能影响全省企业信息安全的重大漏洞和风险。经研判认为可能发生重大及以上企业信息安全事件的信息及时向工业和信息化部、省委省政府报告，同时通报同级数据安全工作协调机制、网信、公安部门，由工业和信息化部统一部署发布红色或橙色预警。经研判认为需要发布黄色预警的，由省工业和信息化厅发布，并向工业和信息化部报备。

各地市工业和信息化主管部门根据本地区工业和信息化领域企业信息安全监测情况，发现可能影响本地区企业信息安全的重大漏洞和风险后，经研判认为需要发布紫色预警的，由地市工业和信息化主管部门发布，并向省工业和信息化厅报备。经研判认为可能超出本地区应对能力范围的，应及时向省工业和信息化厅、市委市政府报告，同时通报同级数据安全工作协调机制、网信、公安部门。

发布预警信息时，应当包括预警等级、起始时间、可能的影响范围和造成的危害、警示事项、应采取的防范措施、处置时限要求、发布范围和发布机关等（模板见附件 4）。

3.4 预警响应

发布黄色及以下预警后，各级工业和信息化主管部门应当针对即将发生的企业信息安全事件特点和可能造成的危害，采取下列措施:

（1）要求涉及预警信息的企业等相关单位及时收集、报告有关信息，加强信息安全风险监测;

（2）组织企业信息安全应急支撑机构加强预警信息分析评估与事态跟踪，密切关注事态发展，提出下步工作措施;

（3）组织专家加强风险研判及原因、影响等分析，提出应急处置方法和整改措施建议。

发布红色和橙色预警后，除采取上述预警响应措施外，还应当针对即将发生的企业信息安全事件特点和可能造成的危害，采取下列措施:

（1）要求市级工业和信息化主管部门、涉及预警信息

的企业等相关单位加强值班值守，相关人员保持通信联络畅通；

（2）组织研究制定防范措施和应急工作方案，组织专家会商研提意见，协调各方资源，做好各项准备工作；

（3）要求相关企业信息安全应急支撑机构进入待命状态，针对预警信息研究制定应对方案，检查应急设备、软件工具等使用情况，确保处于良好状态。

3.5 预警调整和解除

预警发布部门发布预警后，应当根据事态发展，适时调整预警级别并按照权限重新发布。经研判不可能发生事件或风险已经解除的，应当及时宣布解除预警，并解除已经采取的有关预警响应措施。

4 应急处置

4.1 事件报告

工业和信息化领域企业信息安全事件发生后，事发企业应当立即先行判断，对自判为次级及以上事件的，应当及时报告属地工业和信息化主管部门，不得迟报、谎报、瞒报、漏报。

工业和信息化领域企业信息安全应急支撑机构应当通过多种途径监测、收集企业信息安全事件信息，及时向事发地市工业和信息化主管部门报告。

对于初判为次级事件的，事发地市工业和信息化主管部门应立即报告省工业和信息化厅和市委市政府，同时通报同级数据安全工作协调机制、网信、公安部门，并及时报送后

续处置应对情况，直至处置完毕。**对于初判为较大及以上事件的**，事发地市工业和信息化主管部门应立即报告省工业和信息化厅和市委市政府，同时通报同级数据安全工作协调机制、网信、公安部门；省工业和信息化厅接报后应立即报告省委省政府，同时通报同级数据安全工作协调机制、网信、公安、通信管理部门，并及时报送后续处置应对情况，直至处置完毕。**其中，对于初判为重大及以上事件的**，省工业和信息化厅还应立即向工业和信息化部报告。

报告事件研判信息时，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议等（模板见附件 2）。

如在响应、处置企业信息安全事件时伴生或触发其它领域的安全事件，则按相关领域安全事件应急管理要求启动相应的应急预案，及时处置，并向各相关职能部门报告。

4.2 先行处置

工业和信息化领域企业信息安全事件发生后，事发企业应立即开展应急响应工作，采取应急处置措施，控制事态，消除隐患，同时组织研判，保存证据。

4.3 应急响应

工业和信息化领域企业信息安全事件应急响应分为五级：I 级、II 级、Ⅲ级、IV 级、Ⅴ级，分别对应特别重大、重大、较大、次级和一般工业和信息化领域企业信息安全事件。I 级为最高响应级别。

省工业和信息化厅、各地市工业和信息化主管部门视情

组织企业信息安全应急支撑机构、专家等进行研判，确定事件级别和响应等级，启动应急响应。

（1）Ⅰ级响应

属特别重大工业和信息化领域企业信息安全事件的，根据国家数据安全工作协调机制有关决定或经工业和信息化部网信领导小组批准后启动Ⅰ级响应。

①省工业和信息化厅按照工业和信息化部、省委省政府的工作部署，启动应急预案，进入应急状态，加强值班值守，相关人员保持联络畅通，派员参加工业和信息化部、省委省政府的应急指挥工作。掌握事件动态，收集汇总有关情况，及时将事件情况报告工业和信息化部、省委省政府，同时通报同级数据安全工作协调机制、网信、公安、通信管理部门，指导相关地市工业和信息化主管部门、相关企业开展应对工作。组织工业和信息化领域企业信息安全应急专家队伍和应急支撑机构加强安全事件研判分析，配合开展会商研讨，提出应急处置决策建议并提供应急技术支援。

②事发地市工业和信息化主管部门立即启动本地区应急预案，进入应急状态，加强值班值守，相关人员保持联络畅通，派员参加应急指挥工作；加强事件跟踪监测、研判分析和排查处置，全面了解本地区相关企业受影响情况，及时将事态发展情况上报省工业和信息化厅、市委市政府，同时通报同级数据安全工作协调机制、网信、公安部门。

③涉事企业立即进入应急状态，单位法定代表人或主要负责人牵头组建事件应对工作专班，组织研究应对措施，统

筹开展应急处置工作。单位信息安全工作分管领导对应急工作进行具体部署，组织专班加强值班值守，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，采取有效整改处置措施，并及时向所属地市工业和信息化主管部门汇报工作进展和处置情况。

④工业和信息化领域企业信息安全应急支撑机构进入应急状态，加强值班值守，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

（2）II级响应

属重大工业和信息化领域企业信息安全事件的，根据工业和信息化部统一部署启动II级响应。

①省工业和信息化厅按照工业和信息化部、省委省政府的工作部署，启动应急预案，进入应急状态，相关人员保持联络畅通，派员参加工业和信息化部、省委省政府的应急指挥工作。掌握事件动态，收集汇总有关情况，及时将事件情况报告工业和信息化部、省委省政府，同时通报同级数据安全工作协调机制、网信、公安、通信管理部门，指导相关地市工业和信息化主管部门、相关企业开展应对工作。组织工业和信息化领域企业信息安全应急专家队伍和应急支撑机构加强安全事件研判分析，配合开展会商研讨，提出应急处置决策建议并提供应急技术支援。

②事发地市工业和信息化主管部门立即启动本地区应急预案，进入应急状态，相关人员保持联络畅通，派员参加

应急指挥工作；加强事件跟踪监测、研判分析和排查处置，全面了解本地区相关企业受影响情况，及时将事态发展情况上报省工业和信息化厅、市委市政府，同时通报同级数据安全工作协调机制、网信、公安部门。

③涉事企业立即进入应急状态，单位法定代表人或主要负责人牵头研究应对措施，统筹开展应急处置工作，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，采取有效整改处置措施，并及时向所属地市工业和信息化主管部门汇报工作进展和处置情况。

④工业和信息化领域企业信息安全应急支撑机构进入应急状态，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

（3）III级响应

属较大工业和信息化领域企业信息安全事件的，由省工业和信息化厅会同省数据安全工作协调机制、省委网信办报告省委省政府，在省数据安全工作协调机制、省委网信办统筹下，启动III级响应。

①省工业和信息化厅启动应急预案，进入应急状态，成立工作专班，相关人员保持联络畅通；召开紧急会议，听取各相关方面情况汇报，研究紧急应对措施，对应急处置工作进行决策部署。需要成立现场指挥部的，在现场开设指挥部，并由事发地市工业和信息化主管部门提供现场指挥运作的相关保障。协同同级数据安全工作协调机制、网信、公安、通信管理等部门，开展工业和信息化领域企业信息安全防护

及舆情监测、信息安全违法处置、网络流量管理等工作。指导事发地市工业和信息化主管部门开展企业信息安全应急处置，组织工业和信息化领域企业信息安全应急专家队伍和应急支撑机构加强安全事件研判分析，配合开展会商研讨，提出应急处置决策建议并提供应急技术支援。掌握事件动态，收集汇总有关情况，及时将事件情况报告工业和信息化部、省委省政府，通知可能受影响的其他地市做好企业信息安全应急处置工作。视事件严重程度和涉事企业整改处置情况，评估是否开展现场检查。

②事发地市工业和信息化主管部门立即启动本地区应急预案，进入应急状态，相关人员保持联络畅通，派员参加省工业和信息化厅的应急指挥工作；及时将事态发展情况报告市委市政府，同时通报同级数据安全工作协调机制、网信、公安部门。做好本地区应急处置和支援保障工作，组织涉事企业、企业信息安全应急支撑机构等加强事件跟踪监测、事态研判分析、开展事件排查处置，及时上报事件进展及重要情况。

③涉事企业立即进入应急状态，单位法定代表人或主要负责人牵头研究应对措施，迅速实施应急处置，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，保留网络攻击、网络入侵或网络病毒、数据遭受破坏或泄露的证据等相关信息；迅速采取有效整改处置措施，对相关业务系统应用进行整改加固，根除安全问题，恢复受破坏系统的正常运行和受破坏的工业数据，减少危害

和不良影响，并及时向所属地市工业和信息化主管部门汇报工作进展和处置情况。

④工业和信息化领域企业信息安全应急支撑机构持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

（4）IV级响应

属次级工业和信息化领域企业信息安全事件的，由事发地市工业和信息化主管部门会同市委网信办，报告市委市政府，在同级数据安全工作协调机制、市委网信办统筹下，启动IV级响应。

①事发地市工业和信息化主管部门按本地区应急预案组织做好应急处置工作，及时将事件进展及重要情况上报省工业和信息化厅、市委市政府，同时通报同级数据安全工作协调机制、网信、公安部门。处置中需要省级相关部门支持的，省工业和信息化厅予以协调。

②涉事企业及时将事件情况上报所属地市工业和信息化主管部门，保持联络畅通，积极实施应急处置，开展原因分析，尽快就事件中暴露出的网络弱点和缺陷制定并采取有效整改处置措施，加强企业信息安全防护。

（5）Ⅴ级响应

属一般工业和信息化领域企业信息安全事件的，由涉事企业自行启动Ⅴ级响应。

涉事企业应按照企业信息安全保护相关政策标准及时采取有效措施处置事件，加强企业信息安全防护。

4.4 响应级别调整

涉事企业可根据事态发展等情况，向所属地市工业和信息化主管部门申请调整事件响应级别。

事发地市工业和信息化主管部门根据有关企业的申请情况或者事态发展情况等，报告市委市政府，可适时调整事件响应级别，涉及Ⅰ、II、Ⅲ级响应级别调整的，还应当报告省工业和信息化厅。

省工业和信息化厅根据事发地市工业和信息化主管部门上报情况或者事态发展情况等，可适时调整事件响应级别，并报告省委省政府，涉及 Ⅰ、II 级响应级别调整的还应当报工业和信息化部同意。

4.5 舆情监测

各级工业和信息化主管部门协同同级网信、公安部门组织监测公开信息发布渠道，密切关注工业和信息化领域企业信息安全事件舆情信息，跟踪掌握事件影响程度和范围。

4.6 应急结束

事件的影响和危害得到控制或消除后，I 级响应应当根据国家数据安全工作协调机制有关决定或经工业和信息化部网信领导小组批准后结束；II 级响应由工业和信息化部决定结束；III 级响应由省工业和信息化厅会同省委网信办决定结束，并报工业和信息化部、省委省政府；IV 级响应由事发地市工业和信息化主管部门会同市委网信办决定结束，并报省工业和信息化厅、市委市政府；Ⅴ级响应由涉事企业决定结束。

5 事后总结

次级及以上企业信息安全事件应急工作结束后，涉事企业应当自行组织调查处理和总结评估，及时调查事件的起因、经过、责任，评估事件造成的影响和损失，总结事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急工作结束后5个工作日内形成总结报告（模板见附件3），报所属地市工业和信息化主管部门；所属地市工业和信息化主管部门汇总审核后，在应急工作结束后10个工作日内形成报告报送省工业和信息化厅、市委市政府。**其中较大及以上企业信息安全事件**相关调查总结报告，所属地市工业和信息化主管部门汇总审核后，在2个工作日内形成报告报送省工业和信息化厅、市委市政府；省工业和信息化厅汇总审核后，在3个工作日内形成报告报送工业和信息化部、省委省政府。

6 预防工作

6.1 日常管理

各地市工业和信息化主管部门、各工业和信息化领域企业按职责做好企业信息安全事件日常预防工作，制定和完善工业和信息化领域企业信息安全应急预案，落实工业互联网安全分类分级管理与数据安全分级防护，做好企业信息安全检查、隐患排查、风险评估及容灾备份，指定企业信息安全应急工作联系人，健全工业和信息化领域企业信息安全威胁信息通报机制，及时采取有效措施，减少和避免企业信息安全事件的发生及危害，提高应对企业信息安全事件的能力。

6.2 应急演练

省工业和信息化厅协调有关单位根据工作需要组织演练，检验和完善预案，提高实战能力。各地市工业和信息化主管部门、各重点工业和信息化领域企业结合实际情况定期组织应急演练，并将演练情况报省工业和信息化厅。

6.3 安全诊断服务

省工业和信息化厅组织协调应急支撑机构，定期对重点工业和信息化领域企业网络和信息系统、工控系统开展安全诊断服务，对工业数据处理活动开展风险评估，发现安全问题，通报安全情况，提出整改措施，指导督促企业消除风险隐患，提升信息安全事件应对能力。

各地市工业和信息化主管部门应定期组织企业信息安全检查，发现安全问题并敦促整改，如发现重大安全事件苗头性问题，必须报省工业和信息化厅。

各工业和信息化领域重要及核心数据处理企业、三级工业互联网企业等原则上每年开展一次企业信息安全风险评估和自查自纠，及时发现和排除安全隐患。

6.4 宣传与培训

各级工业和信息化主管部门应充分利用各种传播媒介及其他有效的宣传形式，加强工业和信息化领域企业信息安全事件预防和处置的有关法律、法规和政策的宣传，及时向社会发布与公众有关的警示教育信息。开展企业信息安全应急基本知识和技能的宣传活动和培训工作，深化对应急预案中职责、流程和各项基本要求的了解，提高防范意识和技能。

工业和信息化领域企业应当面向员工加强企业信息安全应急宣传教育和培训，学习了解企业信息安全事件警示教育信息，鼓励开展各种形式的信息安全应急相关竞赛。

6.5 手段建设

各级工业和信息化主管部门统筹建设本地区工业和信息化领域企业信息安全监测预警与应急处置能力，组织相关企业开展信息安全风险和事件监测预警工作，及时开展风险和事件应急处置。

工业和信息化领域企业等应当根据有关法律法规和标准的规定，建立健全信息安全管理制度，建设信息安全应急技术手段，开展企业信息安全风险和事件监测，积极配合各级工业和信息化主管部门开展企业信息安全风险监测和技术能力联动等工作，及时排查安全隐患，采取必要的措施防范、处置企业信息安全风险和事件。

6.6 重点时期的预防措施

在国家、省级重大活动等重点时期，各级工业和信息化主管部门指导工业和信息化领域企业、应急支撑机构等加强企业信息安全监测预警、威胁研判和应急响应，强化风险防范与应对措施。相关重点单位、重点岗位、重点企业加强值班值守。工业和信息化领域企业应对网络和信息系统、工控系统加强巡查巡检，加大企业信息安全风险监测力度。

7 保障措施

7.1 落实工作职责

工业和信息化领域企业要严格落实企业信息安全主体

责任，明确企业法人代表、经营负责人第一责任者的责任，工业和信息化领域国有企业要落实网络安全党委责任制。各级工业和信息化主管部门、各工业和信息化领域企业要按照“谁主管谁负责，谁运营谁负责”的原则，建立健全应急工作机制，把工作责任落实到具体部门、具体岗位和相关责任人。

7.2 技术与人才

各级工业和信息化主管部门与其他相关部门加强沟通协调，支持相关企业、科研院所、高等学校开展应急技术攻关、产品服务和能力供给，培养信息安全应急技术人才，形成应急响应工作合力。

省工业和信息化厅积极吸收引进信息安全领域和行业领域专家，统筹纳入广东省工业和信息化领域企业信息安全应急专家队伍，协助各地市工业和信息化主管部门开展企业信息安全应急管理工作。各地市工业和信息化主管部门可组建本地区企业信息安全应急专家队伍。

各工业和信息化领域企业应当加大信息安全投入，配备必要的信息安全专家和专业技术人才，并加强与各应急支撑机构的沟通、协调，建立必要的信息共享机制。

7.3 物资与经费

各级工业和信息化主管部门应综合现有信息化和信息产业等相关领域各类政策和资金渠道，积极支持基础平台建设、技术研发、安全诊断、监测预警、应急演练、物资保障、宣贯培训等工作开展，为企业信息安全日常管理和应急工作提供必要的经费支持。工业和信息化领域企业应当安排必要

的专项资金，支持本单位信息安全应急队伍建设、手段建设、应急演练、应急培训等工作开展。

7.4 保密管理

各级工业和信息化主管部门、应急支撑机构工作人员、应急专家等对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

8 附则

8.1 预案解释

本预案根据实际情况并配合相关法律法规适时组织修订，由省工业和信息化厅负责解释。

8.2 排除条款

涉及军事、国家秘密信息等工业和信息化领域企业信息安全事件应急响应的，按照国家有关规定执行。

涉及关键基础设施、国防科技工业、电力能源、烟草、无线电、电信领域信息安全事件应急响应的，由网信、国防科技工业、能源、烟草专卖、无线电、通信等管理部门另行规定。

8.3 实施时间

本预案自 2026 年 10 月 1 日起实施。

附件 1

工业和信息化领域企业信息安全事件分级

一、符合下列情形之一的，为特别重大工业和信息化领域企业信息安全事件

（一）重要数据、核心数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁的;

（二）工业和信息化领域企业的工业控制系统、工业互联网等网络和信息系统遭受特别重大损害，或工业领域数据遭篡改、破坏、泄露或者非法获取、非法利用，对企业生产运营等造成特别重大损害，导致大范围停工停产、大量业务处理能力丧失等的;

（三）事件对经济建设、社会秩序、公共利益、环境安全和人员生命造成特别严重损害，或可能导致 10 亿元（含）以上直接经济损失的;

（四)发生特别严重个人信息安全事件,涉及 1 亿人(含）以上个人信息或者 1000 万人（含）以上敏感个人信息的;

（五）其他造成或可能造成特别重大危害或影响的。

二、符合下列情形之一且未达到特别重大工业和信息化领域企业信息安全事件的，为重大工业和信息化领域企业信息安全事件

（一）重要数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、社会秩序、经济建设和公众利益构

成严重威胁的;

（二）工业和信息化领域企业的工业控制系统、工业互联网等网络和信息系统遭受重大损害，或工业领域数据遭篡改、破坏、泄露或者非法获取、非法利用，对企业生产运营等造成重大损害，导致较大范围停工停产、较大量业务处理能力丧失等的，事件影响向省外扩散;

（三）事件对经济建设、社会秩序、公共利益、环境安全和人员生命造成严重损害，或可能导致 1 亿元（含）以上 10 亿元以下直接经济损失的;

（四）发生严重个人信息安全事件，涉及 1000 万人（含）以上 1 亿人以下个人信息或者 100 万人（含）以上 1000 万人以下敏感个人信息的;

（五）其他造成或可能造成重大危害或影响的。

三、符合下列情形之一且未达到重大工业和信息化领域企业信息安全事件的，为较大工业和信息化领域企业信息安全事件

（一）重要数据或一般数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、社会秩序、经济建设和公众利益构成较严重威胁的;

（二）工业和信息化领域企业的工业控制系统、工业互联网等网络和信息系统遭受较大损害，或工业领域数据遭篡改、破坏、泄露或者非法获取、非法利用，对企业生产运营等造成较大损害，导致部分业务处理能力丧失等的，事件影响省内多个地市;

（三）事件对经济建设、社会秩序、公共利益、环境安全和人员生命造成较严重损害，或可能导致8000万元（含）以上1亿元以下直接经济损失的;

（四）发生较严重个人信息安全事件，涉及500万人（含）以上1000万人以下个人信息或者50万人（含）以上100万人以下敏感个人信息的;

（五）其他造成或可能造成较大危害或影响的。

四、符合下列情形之一且未达到较大工业和信息化领域企业信息安全事件的，为次级工业和信息化领域企业信息安全事件

（一）数据遭到篡改、破坏、泄露或者非法获取、非法利用，对社会秩序、经济建设和公众利益构成较轻威胁的;

（二）工业和信息化领域企业的工业控制系统、工业互联网等网络和信息系统遭受一定损害，或工业领域数据遭篡改、破坏、泄露或者非法获取、非法利用，对工业生产运营等造成一定损害的，事件影响某个地市;

（三）事件对经济建设、社会秩序、公共利益、环境安全和人员生命造成一定损害，或可能导致5000万元（含）以上8000万元以下直接经济损失的;

（四）发生个人信息安全事件，涉及100万人（含）以上500万人以下个人信息或者10万人（含）以上50万人以下敏感个人信息的;

（五）其他造成或可能造成一般危害或影响的。

五、符合下列情形之一且未达到次级工业和信息化领域

企业信息安全事件的，为一般工业和信息化领域企业信息安全事件

（一）数据遭到篡改、破坏、泄露或者非法获取、非法利用，对企业内部生产经营活动产生威胁的；

（二）工业和信息化领域企业的工业控制系统、工业互联网等网络和信息系统遭受较轻损害，或工业领域数据遭篡改、破坏、泄露或者非法获取、非法利用，对企业生产运营等造成较轻损害的，事件影响企业内部经营管理；

（三）事件影响对企业的合法权益及重要财产造成一定损害，或可能导致5000万元以下直接经济损失的；

（四）发生个人信息安全事件，涉及100万人以下个人信息或者10万人以下敏感个人信息的；

（五）其他造成或可能造成较轻危害或影响的。

附件 2

工业和信息化领域企业信息安全事件报告（模板）

上报单位情况	单位全称	xx
	联系人	xx
	联系方式	xx（手机号）
事件基本情况	发生时间	xx 年 xx 月 xx 日 xx 时 xx 分
	获悉渠道	□自主监测发现 □网上公开发布（URL） □第三方报送（报送单位） □其他（xx）
	涉事单位	xx（单位全称）
	事件级别	□一般 □次级 □较大 □重大 □特别重大
	涉及系统	xx（系统/平台全称）
		IP/域名/URL：xx
	事件原因	（简要描述事件发生原因）
事件涉及数据情况	类型	□研发 □生产 □管理 □运维 □服务
	数据级别	□一般 □重要 □核心
	影响规模	□xx 家企业/xx 个系统平台设备 □xxGB/xx 条数据

	个人信息情况	□个人信息 xxGB/xx 条 □敏感个人信息 xxGB/xx 条 □无
事件影响情况	影响主体	xx（单位全称）
	直接经济损失	xx 万元(需简述初步判定原因及具体情况）
	影响范围及危害	xx 地区/行业(需简要描述初步判定的影响范围及危害）
事件处置建议	1.xx 2.xx ..... （简要描述事件已采取的措施、拟进一步采取的措施和有关建议，以及请求支援事项等。）	

签字（或盖章）：

注：1.涉及系统、影响主体和范围等信息不明确的，可填“尚不明确”。

2.较大及以上企业信息安全事件需上报人签字或上报单位盖章。

附件 3

工业和信息化领域企业信息安全事件
应急处置工作总结报告
（模板）

填 报 单 位：_____（加盖公章）

填 报 日 期：_____年_____月_____日

填 写 说 明

1. 报告材料应客观、真实，不得弄虚作假，不涉及国家秘密，填报单位对所提交材料的真实性负责。

2. 本报告除表格外，其他各项填报要求：A4 幅面编辑，正文应采用仿宋_GB2312 三号字，单倍行间距，两端对齐，一级标题三号黑体，二级标题为三号楷体_GB2312 加粗。

3. 需在报告首页加盖公章。

4. 本报告未经允许不得公开。

一、事件基本情况

（包括工业和信息化领域企业信息安全事件的起因、经过、真实性、责任落实等情况，评估事件造成的影响和损失等）

二、已采取的处置措施

（包括涉事企业在管理制度、技术保护、人员管理等方面采取的处置措施，以及针对本次信息安全事件可能造成的危害已采取的应急手段、用户合法权益保护告知情况等）

三、后续提升改进计划

（包括针对相关工业和信息化领域企业信息安全事件情况，进一步提升企业信息安全保护能力的相关措施）

四、工作经验总结

（针对此类工业和信息化领域企业信息安全事件，总结分析事件防范和应急处置工作的经验教训等）

五、其他事项

（其他需补充说明的事项）

注：请随附工业和信息化领域企业信息安全事件应急处置相关证明材料

附件 4

关于工业和信息化领域企业信息安全风险漏洞的预警通报（模板）

一、预警基本情况

（包括工业和信息化领域企业信息安全风险漏洞的预警等级、起始时间、可能影响的范围和造成的危害、警示事项等）

二、处置措施建议

（包括应采取的处置措施建议，处置时限要求等）

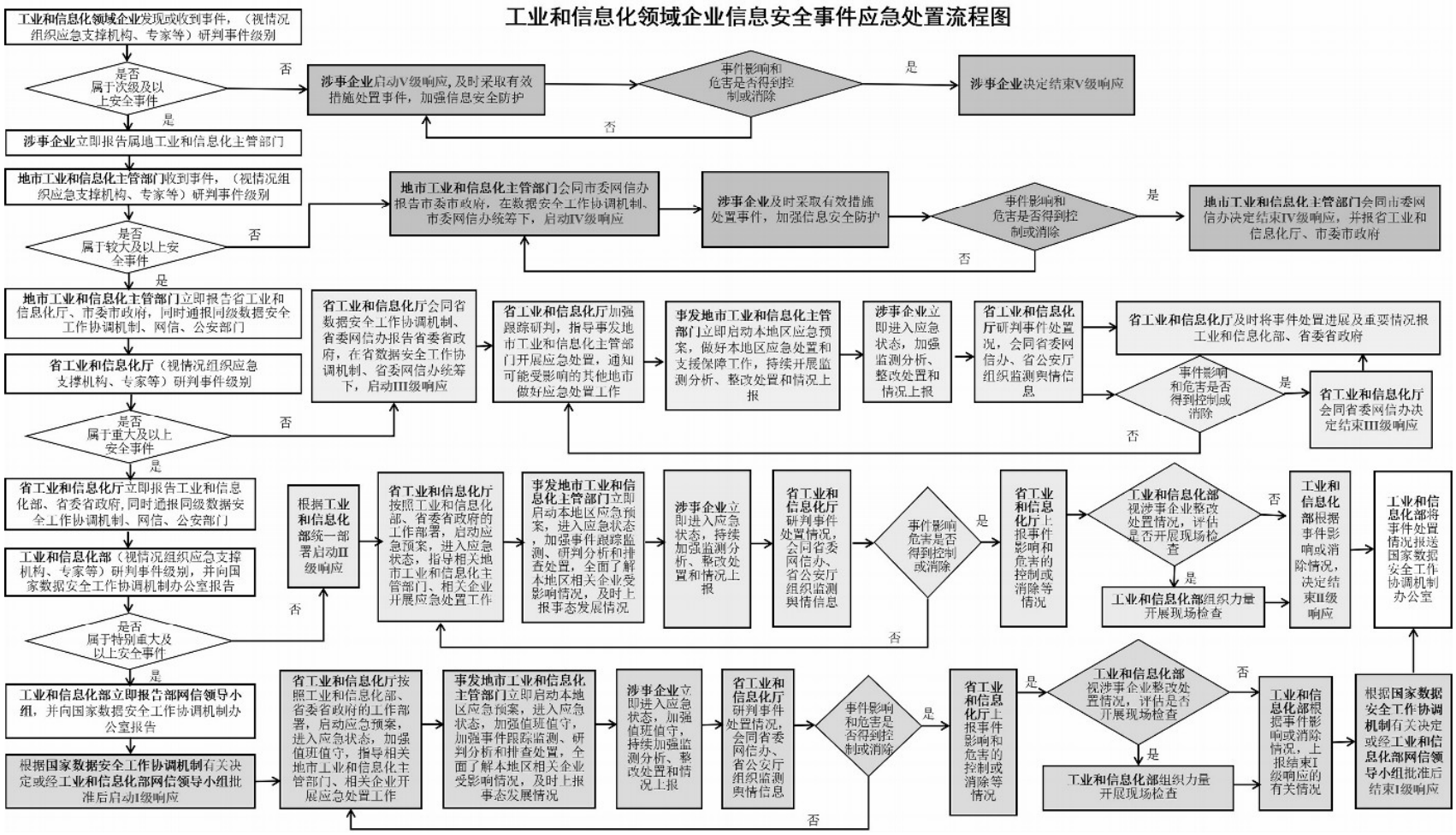
三、发布范围

（包括预警发布范围、发布机关、发布时间等）

四、其他事项

（其他需补充说明的事项）

附件 5


工业和信息化领域企业信息安全事件应急处置流程图
工业和信息化领域企业发现或收到事件，（视情况组织应急支撑机构、专家等）研判事件级别
是否属于次级及以上安全事件
否
是
涉事企业启动V级响应，及时采取有效措施处置事件，加强信息安全防护
事件影响和危害是否得到控制或消除
是
否
涉事企业决定结束V级响应
涉事企业立即报告属地工业和信息化主管部门
地市工业和信息化主管部门收到事件，（视情况组织应急支撑机构、专家等）研判事件级别
是否属于较大及以上安全事件
否
是
地市工业和信息化主管部门会同市委网信办报告市委市政府，在数据安全工作协调机制、市委网信办统筹下，启动Ⅳ级响应
涉事企业及时采取有效措施处置事件，加强信息安全防护
事件影响和危害是否得到控制或消除
是
否
地市工业和信息化主管部门会同市委网信办决定结束Ⅳ级响应，并报省工业和信息化厅、市委市政府
地市工业和信息化主管部门立即报告省工业和信息化厅、市委市政府，同时通报同级数据安全工作协调机制、网信、公安部门
省工业和信息化厅（视情况组织应急支撑机构、专家等）研判事件级别
是否属于重大及以上安全事件
否
是
省工业和信息化厅会同省数据安全工作协调机制、省委网信办报告省委省政府，在省数据安全工作协调机制、省委网信办统筹下，启动Ⅲ级响应
省工业和信息化厅加强跟踪研判，指导事发地市工业和信息化主管部门开展应急处置，通知可能受影响的其他地市做好应急处置工作
事发地市工业和信息化主管部门立即启动本地区应急预案，做好本地区应急处置和支援保障工作，持续开展监测分析、整改处置和情况上报
涉事企业立即进入应急状态，加强监测分析、整改处置和情况上报
省工业和信息化厅研判事件处置况，会同省委网信办、省公安厅组织监测舆情信息
省工业和信息化厅及时将事件处置进展及重要情况报工业和信息化部、省委省政府
事件影响和危害是否得到控制或消除
是
否
省工业和信息化厅会同省委网信办决定结束Ⅲ级响应
省工业和信息化厅立即报告工业和信息化部、省委省政府，同时通报同级数据安全工作协调机制、网信、公安部门
工业和信息化部（视情况组织应急支撑机构、专家等）研判事件级别，并向国家数据安全工作协调机制办公室报告
是否属于特别重大及以上安全事件
否
是
根据工业和信息化部统一部署启动Ⅱ级响应
省工业和信息化厅按照工业和信息化部、省委省政府的工作部署，启动应急预案，进入应急状态，指导相关地市工业和信息化主管部门、相关企业开展应急处置工作
事发地市工业和信息化主管部门立即启动本地区应急预案，进入应急状态，加强事件跟踪监测、研判分析和排查处置，全面了解本地区相关企业受影响情况，及时上报事态发展情况
涉事企业立即进入应急状态，持续加强监测分析、整改处置和情况上报
省工业和信息化厅研判事件处置情况，会同省委网信办、省公安厅组织监测舆情信息
事件影响危害是否得到控制或消除
是
否
省工业和信息化厅上报事件影响和危害的控制或消除等情况
工业和信息化部视涉事企业整改处置情况，评估是否开展现场检查
否
是
工业和信息化部组织力量开展现场检查
工业和信息化部根据事件影响或消除情况，决定结束Ⅱ级响应
工业和信息化部将事件处置情况报送国家数据安全工作协调机制办公室
工业和信息化部立即报告部网信领导小组，并向国家数据安全工作协调机制办公室报告
根据国家数据安全工作协调机制有关决定或经工业和信息化部网信领导小组批准后启动Ⅰ级响应
省工业和信息化厅按照工业和信息化部、省委省政府的工作部署，启动应急预案，进入应急状态，加强值班值守，指导相关地市工业和信息化主管部门、相关企业开展应急处置工作
事发地市工业和信息化主管部门立即启动本地区应急预案，进入应急状态，加强值班值守，加强事件跟踪监测、研判分析和排查处置，全面了解本地区相关企业受影响情况，及时上报事态发展情况
涉事企业立即进入应急状态，加强值班值守，持续加强监测分析、整改处置和情况上报
省工业和信息化厅研判事件处置情况，会同省委网信办、省公安厅组织监测舆情信息
事件影响和危害是否得到控制或消除
是
否
省工业和信息化厅上报事件影响和危害的控制或消除等情况
工业和信息化部视涉事企业整改处置情况，评估是否开展现场检查
否
是
工业和信息化部组织力量开展现场检查
工业和信息化部根据事件影响或消除情况，上报结束Ⅰ级响应的有关情况
根据国家数据安全工作协调机制有关决定或经工业和信息化部网信领导小组批准后结束Ⅰ级响应

公开方式：主动公开