白银矿冶职业技术学院

网络安全应急响应和事故上报制度

2019 年 11 月

目　录

1 总则

1.1 编制目的

为了提高白银矿冶职业技术学院处置网络、信息系统的安全突发事件的能力，最大限度地预防和减少网络、信息系统安全突发事件及其造成的损害和影响，保障局网络、信息系统的安全稳定运行，维护正常的生产秩序，制定本制度。

1.2 编制依据

本制度依据以下法律法规、标准制度及相关制度，结合白银矿冶职业技术学院实际制定。

1） GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

2） GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理指南

1.3 适用范围

1.3.1 本制度适用于白银矿冶职业技术学院应对和处置各类对白银矿冶职业技术学院网络、信息系统造成严重损失和影响的突发事件。

1.3.2 本制度用于指导和规范本局制定网络、信息系统突发事件处置预案，建立分级负责的网络、信息系统突发事件应急处置体系，规范处理突发网络、信息事件的逐级汇报流程。单位应按照“谁主管、谁负责，谁运行、谁负责”的原则，制定网络、信息系统安全应急预案。

2 应急处置基本原则

2.1 预防为主，常备不懈，超前预想。

做好应对网络信息系统突发事件的预案准备、应急资源准备、保障措施准备和超前信息系统突发事件预想，充分利用现有资源，制定科学的应急预案，定期组织开展应急培训和应急演练，提高对各类事件的应急响应和综合处理能力。

2.1 安全第一、预防为主。

坚持“安全第一、预防为主”的安全方针，立足安全防护，加强预警，重点保护基础信息网络和主营业务信息系统；建立预防和预警机制，将风险评估和安全检查列入常态工作，制定信息通报工作制度，做到早发现、早报告、早处置。

2.2 统一领导、分级负责。

按照“谁主管、谁负责，谁运营、谁负责”的要求，实行“统一领导、分级

负责、各司其职、协调配合”，建立健全信息系统安全突发事件应急处置工作责任制，明确责任，并将责任落实到人。

2.3 处置优先、快速反应。

发生信息系统安全突发事件时，要按照处置优先、快速反应原则，及时获取充分而准确的信息，跟踪研判，果断决策，按照相关应急预案进行迅速处置，最大程度地减少危害和影响。

2.4 科学化、规范化。

加强技术储备，规范应急处置措施与操作流程，实现信息系统安全突发事件应急处置工作的科学化与规范化。树立常备不懈的观念，定期进行预案演练，确保应急预案切实可行。

3 应急指挥机构及职责

3.1 应急指挥机构

3.1.1 白银矿冶职业技术学院信息系统安全应急指挥部（以下简称“应急指挥部”）是白银矿冶职业技术学院网络信息系统突发事件应急工作的管理决策机构。

总指挥由分管信息的总工担任，指挥部成员包括白银矿冶职业技术学院信息中心、突发事件相关业务部门领导和有关人员。

3.1.2 白银矿冶职业技术学院信息中心，负责单位网络信息系统突发事件应急的日常管理工作。

3.2 应急指挥机构的职责

3.2.1 应急指挥部在信息系统应急工作中的主要职责：

（1） 贯彻落实国家、行业、白银矿冶职业技术学院有关网络信息系统突发事件应急处理的法规、规定；

（2） 研究信息系统重大应急决策和部署；

（3） 宣布进入和解除应急状态，决定实施和终止信息系统安全应急预案。

（4） 统一领导、指挥单位信息系统Ⅰ级、Ⅱ级和III级突发事件的应急处置工作。

3.2.2 白银矿冶职业技术学院信息中心在信息系统安全应急工作中的主要

职责：

（1） 监督执行应急指挥部下达的应急指令、重大应急决策和部署，协调各方应急资源，组织应急处置；

（2） 组织制定网络信息系统应急工作相关制度、标准、规范和预案，定期组织评估、修订和复核，并监督、检查贯彻执行情况；

（3） 及时了解和掌握网络信息系统突发事件与应急处置工作情况，向单位应急指挥部报告应急处置过程中发现的重大问题，并协调解决；

（4） 按相关规定参与、组织网络信息系统事件调查、总结应急处理经验和教训等后期处置工作。

4 应急响应

4.1 事件类型

信息系统系统存在受到计算机病毒、漏洞攻击、扫描窃听以及设备设施故障等风险，上述风险引起的信息安全突发事件主要包括：

（1）有害程序类突发事件：指受到有害程序的影响而导致的信息安全突发事件。有害程序类事件包含计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件等。

（2）网络攻击类突发事件：指通过网络或其它技术手段，利用配置缺陷、协议缺陷、程序缺陷等攻击信息系统，造成信息系统异常或不可用的信息安全突发事件。网络攻击类事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件等。

（3）信息破坏类突发事件：指通过网络或其它技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致系统瘫痪、数据毁坏、数据泄密的信息安全突发事件。信息破坏类事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件等。

（4）信息内容安全类突发事件：指利用网络发布或传播危害国家安全、社会稳定和公共利益的内容的信息安全突发事件。信息内容包括违反宪法和法律、行政法规的信息，组织串连、煽动集会游行的信息等。

（5）故障类突发事件：指信息系统系统因自身或外围设备设施故障、以及人为误操作等导致的信息安全突发事件。故障类事件包括软硬件自身故障、外围

保障设施故障、人为破坏事故、人为误操作事故等。

（6）灾害类突发事件：指由于不可抗力对信息系统系统造成物理破坏而导致的信息安全突发事件。灾害类事件包括水灾、台风、冰灾、火灾、雷击、地震、坍塌、恐怖袭击、战争等导致的信息安全突发事件。

单位基础设施类信息系统面临的风险主要包括网络攻击类突发事件、故障类突发事件和灾害类突发事件等；管理信息系统面临的风险主要包括：有害程序类突发事件、信息破坏类突发事件、故障类突发事件和灾害类突发事件等；信息发布和传播系统面临的风险主要包括：有害程序类突发事件、网络攻击类突发事件、信息内容安全类突发事件和故障类突发事件等。

4.2 事件分级

根据网络信息系统突发事件对服务的社会用户和白银矿冶职业技术学院生产、经营和管理的影响范围、严重程度、可能产生的后果和损失等因素，将信息系统事件分为Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）、Ⅳ级（一般）。

4.2.1 特别重大突发事件（Ⅰ级）

指信息系统安全突发事件造成单位网络大面积中断、或主营业务系统大面积瘫痪，对单位造成巨大经济损失或产生严重不良社会影响的：

（1）网络大面积中断：因网络中断，造成单位内三分之二以上部门不能正常使用一个及以上的主营业务系统，持续时间达 12 小时以上的。

（2）主营业务系统大面积瘫痪：因系统主要功能不可用，造成单位内三分之二以上部门不能正常使用一个及以上主营业务系统，系统瘫痪时间 12 个小时以上的。

4.2.2 重大突发事件（Ⅱ级）

指信息系统安全突发事件造成单位网络较大面积中断、或主营业务系统较大面积瘫痪，对单位造成重大经济损失的或产生较严重不良社会影响。

（1）网络较大面积中断：因网络中断，造成单位内半数以上部门不能正常使用一个及以上主营业务系统，持续时间超过 6 小时以上。

（2）主营业务系统较大面积瘫痪：因系统主要功能不可用，造成单位内半数以上部门不能正常使用一个及以上主营业务系统，系统瘫痪时间 6 个小时以上。

4.2.3 较大突发事件（Ⅲ级）

指信息系统安全突发事件造成单位网络中断、或主营业务系统瘫痪、或主营业务系统数据毁坏、或经营管理数据泄密，或信息系统发布和传播系统发生政治敏感信息事件，对单位造成较大经济损失或产生一定程度不良社会影响的。

（1）网络中断：因综合业务数据网络中断，造成单位内四分之一以上部门不能正常使用一个及以上主营业务系统，持续时间超过 2 小时以上。

（2）主营业务系统瘫痪：因系统主要功能不可用，造成单位内四分之一以上部门不能正常使用一个及以上主营业务系统，系统瘫痪时间 2 个小时以上。

（3）数据毁坏：主营业务数据毁坏后不能恢复的。

（4）数据泄密：发生涉及单位秘密的数据泄漏。

（5）政治敏感信息事件：单位门户网站被篡改或企业邮件系统被不法份子利用，发布或传播了政治敏感信息，造成了一定程度不良政治影响的。

4.2.4 一般突发事件（Ⅳ级）

指信息系统安全突发事件造成单位网络中断、或主营业务系统瘫痪、或部分主营业务系统数据毁坏，对单位造成一定的经济损失。

（1）网络中断：因综合业务数据网络中断而不能正常使用网络，造成单位内 1 个及以上部门不能正常使用一个及以上主营业务系统，持续时间超过 1 小时以上。

（2）主营业务系统瘫痪：因系统主要功能不可用，造成单位内 1 个及以上部门不能正常使用一个及以上主营业务系统，系统瘫痪时间 1 个小时以上。

（3）数据毁坏：主营业务数据毁坏后只能部分恢复的。

4.3 先期处置

4.1.1 信息系统安全应急处置按照各专业协同处理的原则进行，需要内部多个部门专业协同处置或外部应急资源支持的应急事件，由应急指挥部负责统一协调。

4.1.2 单位应密切关注突发事件情况与先期处置效果，责成各职能管理部门开展各项应急准备前期工作，有关职能管理部门组织、指挥、调度相关应急力量及时隔离故障区域，初步收集受损情况，并主动与白银矿冶职业技术学院领导层或国家有关部门联系沟通，及时汇总并上报。

4.3 应急响应

4.3.1 Ⅰ级响应

发生Ⅰ级突发事件，或II级突发事件演化为Ⅰ级突发事件，启动Ⅰ级响应。

单位在白银矿冶职业技术学院的总体协调、指导下进行Ⅰ级响应。

（1）应急指挥部总指挥下令，白银矿冶职业技术学院信息中心发布应急响应启动令，并报白银矿冶职业技术学院。

（2）应急指挥部总指挥、副总指挥、单位联络员以及联络员全天候值班，信息系统管理职能部门负责人、与应急相关的其他部门负责人以及相关设备厂商或系统开发商责任人就位，取消休假，处于随时待命状态。

（3）应急指挥部通知受影响应用系统的业务主管部门，启动对应业务的单项应急预案或临时应急措施，必要时临时用人工方式处理业务。

（4）根据白银矿冶职业技术学院信息中心的要求，调派相关网络信息技术专家参与现场工作组的工作。

（5）白银矿冶职业技术学院信息中心随时收集、整理应急救援情况的信息，以专报方式每天报送白银矿冶职业技术学院应急指挥机构，直到应急结束。

4.3.2 II级响应

在白银矿冶职业技术学院的总体协调、指导下进行Ⅱ级响应。

（1）应急指挥部起文发布应急响应启动令。

（2）应急指挥部总指挥或副总指挥、单位联络员以及联络员全天候值班，信息系统管理职能部门负责人、与应急相关的其他部门负责人以及相关设备厂商或系统开发商责任人就位，取消休假，处于随时待命状态。

（3）应急指挥部通知受影响应用系统的业务主管部门，启动对应业务的单项应急预案或临时应急措施，必要时临时用人工方式处理业务。

（4）应急指挥部调派相关网络信息技术专家参与现场督导组或专家组的工作。

（5）白银矿冶职业技术学院信息中心随时收集、整理应急救援情况的信息，以专报方式每天报送白银矿冶职业技术学院应急指挥机构，直到应急结束。

4.3.3 III级响应

（1）联络员全天候值班，与应急相关的人员就位，取消休假，处于随时待

命状态。

（2）应急指挥部通知受影响应用系统的业务主管部门，启动对应业务的单项应急预案或临时应急措施。

（3）必要时调派相关网络信息技术专家组成专家组赴现场参与应急处置工作。

（4）白银矿冶职业技术学院信息中心随时收集、整理应急处置情况的信息，并每天向单位应急指挥部报告一次，直到应急结束。

4.3.4 IV 级响应

发生 IV 级突发事件，启动 IV 级响应。

应急指挥部组织相关的应急处置工作，组织技术人员现场处理故障，同时根据事件发生范围、严重程度、发展趋势等做出预警信息发布和上报工作，通知相关部门做好应急准备。事件应急工作组其他成员按照职责分工，做好相应工作。应急结束后向单位应急指挥部汇报事件处置情况。

4.4 响应调整

单位应急指挥部视事件发展情况、危害程度、事件分级条件等综合因素研究决定是否调整事件响应。

4.5 应急结束

7.5.1 在同时满足下列条件下，事件提请应急指挥部部解除应急状态：

（1） 网络信息系统突发事件已得到有效控制，情况趋缓。

（2） 网络信息系统突发事件处置结束，网络信息系统恢复正常运行。

（3） 白银矿冶职业技术学院信息中心发布的解除应急响应状态的指令。

7.5.2 应急部门应及时向现场应急指挥部和参与应急支援的人员传达解除应急状态响应的指令，恢复正常生产秩序。

7.5.3 应及时向上级有关部门和单位应急指挥机构报告已解除应急状态，恢复正常生产秩序。

5 事件上报

5.1 发生网络信息系统突发事件时，由白银矿冶职业技术学院信息中心报

告。

5.2 建立突发事件报告制度。报告分为紧急报告和详细汇报。紧急报告是指事件发生后，白银矿冶职业技术学院信息中心向应急指挥部以口头和应急报告表形式汇报事件的简要情况；详细汇报是指由信息中心在事件处理暂告一段落后，以书面形式提交的详细报告。

5.3 白银矿冶职业技术学院信息中心对各类突发事件的影响进行初步判断，I 级事件应在 30 分钟内向单位应急指挥部进行报告，II 级事件应在 2 小时内向单位应急指挥部进行报告，III 级事件在 8 小时内向单位应急指挥部进行汇报，IV 级事件在 24 小时内向白银矿冶职业技术学院信息中心进行汇报。

5.4 任何科室和个人均不得缓报、瞒报、谎报或者授意他人缓报、瞒报、谎报事件。

5.5 要规范口头报告的内容和格式，要求内容简洁、清楚、准确。口头报告的内容主要包括事件发生的时间、概况、可能造成的影响等情况。口头报告后应以传真方式报送白银矿冶职业技术学院信息系统应急报告表。

6 后期处置

6.1 事件监测

Ⅰ级网络信息系统突发事件应急处理结束后应安排专人密切关注、监测系统 2 周，确认无异常现象。Ⅱ级网络信息系统突发事件应急处理结束后应安排专人密切关注、监测系统 1 周，确认无异常现象。Ⅲ、Ⅳ级网络信息系统突发事件应急处理结束后应安排专人密切关注、监测系统 2 天，确认无异常现象。

6.2 事件调查

6.2.1 突发事件应急处理结束后，应按照单位信息系统事故调查相关要求，组成事件调查组对事件进行调查，形成事件调查报告，交由白银矿冶职业技术学院信息中心按规定上报备案。调查要准确、及时、公正地查清事件性质、原因和责任，总结经验教训，提出防范措施，并对责任者提出处理意见。除组织内部调查以外，应积极配合政府有关部门组织的调查。

6.2.2 按照单位规定自行组织调查的，应负责查清事故原因，评估事件影响，认定事件责任，提出整改措施，并将网络信息系统突发事件事故调查报告报白银矿冶职业技术学院信息中心，并通报事故调查、处理情况。

6.3 总结及改进

6.3.1 应客观、公正、准确地查清事故原因、发生过程、恢复情况、事故损失等，认定责任，提出整改措施。

6.3.2 应组织研究网络信息系统各类突发事件发生的原因和特点，综合分析网络信息系统中存在的关键点和薄弱点，及时总结应急响应工作的经验和教训，提出整改措施，制定整改实施方案并予以落实，整改措施和方案应报白银矿冶职业技术学院信息中心备案。

6.4 奖惩

6.4.1 按照白银矿冶职业技术学院有关要求，对网络信息突发事件应急管理工作中做出突出贡献的先进集体和个人，给予表彰和奖励。

6.4.2 对迟报、谎报、瞒报和漏报网络信息系统突发事件，或应急管理工作中有失职、渎职行为的人员按照国家和单位有关要求给予警告、通报批评、责令改正。造成严重危害后果的，视情给予行政处分；构成犯罪的，依法追究刑事责任。

7 附则

7.1 预案报备

网络信息系统突发事件处置专项预案须报白银矿冶职业技术学院信息中心备案，备案材料至少应包括有关的备案申请表、评审意见、文本目录、电子文档等各种配套材料。

7.2 制度修订

7.2.1 根据国家和白银矿冶职业技术学院相关法律法规要求，及时修订完善本预案。

7.2.2 本制度至少每三年修订一次，修订结果应进行详细记录，留存相关文档。应结合实际情况，建立应急预案修订机制。

7.2.3 有下列情形之一的，应组织对应急预案进行修订：

（1） 企业生产规模发生较大变化或进行重大技术改造的；

（2） 企业隶属关系发生变化的；

（3） 周围环境发生变化、形成重大危险源的；

（4） 应急指挥体系、主要负责人、相关部门人员或职责已经调整的；

（5） 依据的法律、法规和标准发生变化的；

（6） 应急预案演练、实施或应急预案评估报告提出的重大整改要求；

7.3 制定与解释

本制度由白银矿冶职业技术学院信息中心制定并负责解释。