# 日照职业技术学院办公室文件

日职院办字〔2019〕31号

## 关于印发《日照职业技术学院网络信息安全事件应急预案》的通知

学校各单位:

为加强学校网络安全管理，规范网络安全事件处置程序，明确网络安全事件处置工作责任，学校制定了《日照职业技术学院网络信息安全事件应急预案》，现印发给你们，请认真学习，并遵照执行。

党委（学院）办公室

2019年11月20日

# 日照职业技术学院
# 网络信息安全事件应急预案

## 1. 总则

### 1.1 编制目的

全面加强日照职业技术学院网络安全管理，规范网络安全事件处置程序，明确网络安全事件处置工作责任，对各类涉及学校的网络安全突发事件及时作出响应和处置，把各方面损失降到最低。

### 1.2 编制依据

国家《信息安全技术 信息安全应急响应计划规范(GB/T 24363-2009)》《信息安全技术 信息安全事件分类分级指南（GB/Z 20986—2007）》等标准及上级有关文件精神。

### 1.3 适用范围

本预案适用于日照职业技术学院所属网站、信息系统、服务器、计算机等发生的网络与信息安全类突发事件（包括但不限于黑客攻击或系统漏洞导致的网页篡改、信息泄露、远程控制、木马病毒传播等）的应急处置工作。

## 2. 组织机构与职责

### 2.1 网络安全与信息化工作领导小组

贯彻落实上级关于加强网络安全管理的有关精神，研究审议学校信息安全规章制度，健全网络安全工作体系；对学校网络信息安全中的重大问题进行审议和决策；监督各单位网络信息安全措施的落实情况；对重大安全责任事件中的失职渎职和违纪违规人员依相关规定作出追责问责处理。

2.2 网络安全与信息化工作领导小组办公室

贯彻落实学校网络安全与信息化工作领导小组的各项决策，牵头抓好学校各项网络安全制度的落实；按照本预案和有关文件规定，牵头负责学校网络安全日常管理，以及学校公共信息化系统突发网络安全事件的应急处置、善后、事件原因调查等；为学校各责任单位提供必要的网络安全技术支持。

2.3 各网站（系统）责任部门

贯彻落实学校各项网络安全规章制度，做好本部门负责的网站（系统）的日常维护和安全管理；抓好本部门人员网络安全教育培训；发现本部门网站（系统）出现安全漏洞或网络安全事件，按本预案和相关文件要求，负责事件的处置、善后、记录、上报等工作；配合相关部门做好事件原因调查等工作。

## 3. 网络信息安全事件等级确认与划分

根据上级有关文件，结合学校实际，将网络安全事件按严重程度分为四级。

3.1 特别重大事件（I 级）

学校校园网上出现大面积的串联、煽动和蛊惑信息；主页出现反动、煽动民族分裂、破坏稳定等违法信息及链接；网络发现泄密、失密事件。

3.2 重大事件(II级)

影响学校系统正常运转的攻击事件，如财务系统、办公系统相关的攻击；可能造成用户隐私信息窃取、丢失、损坏的漏洞；可由校外访问的页面发生篡改或被替换成非法信息的事件；其它可能对社会公共安全或学校造成危害或不良影响的事件或漏洞。

3.3 较大事件(III级)

校园网主要网络设备和服务器受到非法侵入；网页出现非法信息及链接。

3.4 一般事件(IV级)

影响部门系统正常运转的攻击事件，或可能造成紧急安全事件的漏洞；其他不构成公共危害或社会不良影响的安全事件或漏洞。仅校内访问的页面发生无害篡改、系统或网站隐藏漏洞等事件。

**4. 网络信息安全事件的应急响应处置**

按照网络安全与信息化工作“谁建设谁负责，谁使用谁负责，谁管理谁负责”的原则，学校网络安全事件的应急响应处置采取统一管理、分级负责、快速反应、高效处置的办法，针

对不同等级的网络安全事件启动相应的处置流程。各等级的事件处置流程如下。

4.1 特别重大事件(I 级)处置流程

4.1.1 信息化办公室先行通过技术手段紧急处置。信息化办公室在获悉事件发生后 5 分钟内切断事发网站(系统)的域名解析或 IP 地址，与互联网断开连接；15 分钟内关闭影响安全和稳定的网络设备，断开与破坏来源的网络物理连接；锁定相关服务器、日志文件、程序源码、数据库等备查。

4.1.2 信息化办公室向学校网络安全和信息化工作领导小组组长、副组长报告；

4.1.3 在学校网络安全与信息化工作领导小组指挥下，按照有关规定开展消除漏洞、控制不良影响、追查攻击来源、妥善做好善后、报告上级单位、责任追究等后续处置工作；

4.1.4 事件处理材料归档备查。

4.2 重大事件处置流程(II 级)

4.2.1 信息化办公室第一时间关闭涉事网站（系统）的域名解析，或采取技术措施限制互联网访问；

4.2.2 信息化办公室第一时间通过技术措施，追查锁定破坏来源 IP 并实施限制，避免攻击持续；

4.2.3 通知涉事网站（系统）责任单位和系统管理员，由责任单位在信息化办公室指导下，第一时间组织力量进行安全

处置，修复存在的漏洞，评估造成的损失，做好事件处置记录，处理结果报信息化办公室；

4.2.4 事件处理材料归档备查；

4.2.5 信息化办公室根据事件性质，决定是否上报学校网络安全与信息化工作领导小组研究进一步处理措施。

4.3 较大事件处置流程(III级)

1.信息化办公室第一时间根据事件性质决定是否关闭涉事网站（系统），或采取技术措施限制互联网访问；

2.将事件情况紧急通知信息系统责任单位管理员，同时通报责任单位负责人；

3.责任单位系统管理员及时组织技术力量消除非法信息，恢复系统。做好事件处置记录，处理结果报信息化办公室；

4.事件处理材料归档备查；

5.信息化办公室根据事件性质，决定是否上报学校网络安全与信息化工作领导小组研究进一步处理措施。

4.4 一般事件处置流程(IV 级)

4.4.1 信息化办公室对发现的漏洞进行分类验证，对存在可利用漏洞的业务系统，采取临时性禁止外网访问措施；

4.4.2 信息化办公室将漏洞情况通知责任单位；漏洞详细情况及处理建议发送给责任单位管理员；

4.4.3 责任单位管理员按要求进行漏洞处理，处理完成后

填写反馈报告，报信息化办公室；

4.4.4 信息化办公室根据漏洞修复情况，恢复相关访问权限；

4.4.5 事件处理材料归档。

**5. 附则**

**5.1** 本预案原则上每 3 年修订 1 次，有下列情形之一的，应提前进行修订：

5.1.1 网络安全管理组织机构及其职责发生重大调整的；

5.1.2 依据的法律、行政法规、规章等发生变化的；

5.1.3 网络安全与信息化工作领导小组认为应当修订的。

**5.2** 本预案自印发之日起实施，由信息化办公室负责解释。

日照职业技术学院办公室　　2019 年 11 月 20 日印发