

서울특별시교육청 디지털재난 대비 및 대응 조례안

검 토 보 고

I. 회부경위

1. 의안번호 : 제1705호
2. 발 의 자 : 전병주 의원 등 27명
3. 발의일자 : 2024년 4월 3일
4. 회부일자 : 2024년 4월 8일

II. 제안이유

- 지난해 정부의 행정 전산망 오류로 인해 민원 대란이 발생하며 디지털 재난을 예방 및 대응하기 위한 데이터 및 인프라 관리, 개인정보 보호를 위한 제도 개선의 필요성이 강조되는 상황임.
- 이에 서울시교육청이 보유한 교육 정보에 대한 디지털재난의 대비 및 대응에 관한 사항을 규정하여 안정적인 위기관리 기반 구축을 마련하기 위해 조례를 제정함.

III. 주요내용

1. 조례의 목적과 정의에 대해 규정함(안 제1조~제2조).

2. 디지털재난 대응에 대한 교육감의 책무에 대해 규정함(안 제3조).
3. 디지털재난 대비 및 대응을 위한 기본계획 수립에 관한 사항을 규정함(안 제4조).
4. 디지털재난 대비를 위한 안전점검 및 훈련에 관한 사항을 규정함(안 제5조).

IV. 참고사항

1. 관계법령

- 「재난 및 안전관리 기본법」
- 「정보통신기반 보호법」
- 「개인정보 보호법」
- 「유아교육법」, 「초·중등교육법」
- 「유아교육정보시스템 및 교육정보시스템의 운영 등에 관한 규칙」

2. 예산조치 : 해당없음(비용추계서 비대상사유서 별첨)

3. 기 타

- 입법예고(2024. 4. 12. ~ 4. 16.) 결과 : 의견 없음

V. 검토 의견(수석전문위원 김창범)

1. 제안경위 및 주요내용

- 동 조례안은 2024년 4월 3일 전병주 의원 등 27명에 의해 의안번호 제1705호로 발의되어 2024년 4월 8일 우리 위원회로 회부되었습니다.
- 동 조례안은 서울시교육청의 교육정보시스템을 재난이나 해킹, 컴퓨터 바이러스, 디도스 공격, 기술적 오류 등으로부터 보호하고, 각종 디지털 재난으로 인해 발생하는 피해를 최소화하기 위한 계획의 수립, 안전 점검 및 재난 대비 훈련의 시행 등에 대해 규정하고자 발의되었습니다.

2. 주요 검토의견

가. 제정 취지에 대한 검토

- 국가정보원 국가사이버안보센터는 러시아-우크라이나 전쟁으로 대표되는 국제 정세 변화와 남북관계 악화 등으로 사이버 위협이 증가함에 따라 지난 2022년 3월 21일부터 사이버 위기 경보를 ‘관심’에서 ‘주의’로 상향 조정하였으며, 현재까지 ‘주의’ 정보 단계를 유지하고 있습니다.¹⁾
- 이에 정부는 엄중한 상황 인식 아래 공공이 구축하고 있는 디지털 환경과 인프라가 내·외부적인 위협으로부터 보호받을 수 있도록 적극적인 예방과 보안대책을 전개하기 위해 노력하고 있습니다.
- 그러나 사회 전반의 지능 정보화와 전자정부 시스템의 고도화 등은 범국가적 차원의 디지털 재난 대응을 더욱 어렵게 하고 있으며,

1) 국가정보원, 주요업무 > 사이버안보 > 사이버위기경보
https://www.nis.go.kr/AF/1_7_1_1/list.do (검색일 2024-04-15)

교육 현장에서도 디지털화가 촉진됨에 따라 사이버 위협 등에 대한 대비와 대응에 어려움이 커지고 있습니다.

○ 특히, 교육부와 서울시교육청을 비롯한 교육 당국이 디지털 교과서 도입, 전자철판 보급, AI와 빅데이터 기술 등에 기반한 에듀테크 활용 확대 등을 추진하는 등 디지털 환경 구축에 매진함에 따라 보호해야 할 정보와 인프라의 범위가 급속하게 확대되고 있는 실정입니다.

○ 한편, 지난해부터 경기도교육청 전국학력평가시스템의 개인 성적정보 유출 사건과²⁾ 4세대 교육행정정보시스템(NEIS)의 전산장애 및 문항정보표 유출 사건³⁾ 등이 연이어 발생함에 따라 서울시교육청 차원에서도 디지털 재난 대응의 필요성이 더욱 인식되고 있습니다.

더욱이 ‘서울시교육청 PC 390여 대를 포함한 공공기관 PC 3천여 대가 최근 3년 동안 해커의 공격을 받은 것이 확인되었다’ 라는 내용의 언론 보도를⁴⁾ 통해서도 알 수 있듯이 서울시교육청 역시 디지털 재난의 예외가 될 수 없다는 사실이 확인되고 있습니다.

○ 이러한 상황 속에서 동 조례안은 서울시교육청이 기구축된 디지털 인프라를 기술적·인위적 위협 등으로부터 안전하게 보호될 수 있도록

2) 경기도교육청은 내부 시스템을 통해 관리하는 ‘2022학년도 11월 고2 전국연합학력평가’의 수험생 개인정보 및 성적 정보가 유출되었다고 2023년 2월 19일 발표하였음. 이후 경찰 조사 결과, 2019학년도와 2021학년도 자료까지 총 299만 6,485건의 개인정보가 유출되었던 것으로 확인된 바 있음.

(자료 : 서울시교육청, 공지사항 > “전국연합 학력평가 성적자료 유출 안내”,

https://www.sen.go.kr/user/bbs/BD_selectBbs.do?q_bbsSn=1100&q_bbsDocNo=20230509105039316 (검색일 2024-04-15))

3) 2023년 6월 21일, 학교 및 교육행정기관의 업무 정보를 처리하는 나이스 시스템에 AI, 빅데이터 기술 등을 적용한 4세대 나이스가 개통되었음. 그러나 개통 첫날부터 시스템 속도가 저하되면서 행정업무가 지연되는 등의 문제가 발생하고, 일부 학교의 기말고사(지필평가) 문항정보표(시험문항별 답안지)가 타학교 나이스에서 출력되는 현상이 발생함. 이후 2024년 1월, 연말정산 입력 시작일에 연말정산 시스템에 오류가 발생하는 등의 기술적 문제가 확인되기도 했음.

(자료 : 에듀프레스(2023.6.23.), “다른 학교 시험 답안지까지 유출되는 4세대 나이스..학교 발각”,

<http://www.edupress.kr/news/articleView.html?idxno=10525>; 교육부 설명자료(2023.6.23.), “4세대 나이스 사용 불편함 없도록 시스템 안정화에 최선”, <https://www.korea.kr/news/top50View.do?newsId=148916722> 등)

4) KBS(2024.4.2.), “[단독] “중앙선관위 직원 해킹 당해”...“업무용 PC 정보 털려” [사이버위협]

<https://news.kbs.co.kr/news/pc/view/view.do?ncd=7929654&ref=A> (검색일 2024-04-02)

적극적인 예방과 보안대책을 강구하고자 하는 것으로 입법 취지의 측면에서 바람직한 것으로 생각됩니다.

나. 조례안의 체계와 주요 조문별 검토

1) 조례안의 체계

- 동 조례안은 제1조부터 제3조까지 목적과 정의, 적용범위와 교육감의 책무에 관해 규정하고, 제4조에서 기본계획의 수립과 시행, 제5조에서 안전점검 및 디지털재난 대비 훈련, 제6조에서 디지털재난 발생 시 조치사항 등에 대해 명시하고 있으며, 제7조에서 디지털재난 예방 및 대응 등을 위한 협력체계 구축에 대해 다루고 있습니다.
- 동 조례안은 조문 간 구성과 체계 등에 있어서 「자치법규 입안 길라잡이」와 「알기 쉬운 법령 정비기준」을 준수하고 있다는 점에서 조례 제정에 따른 형식적 문제는 없는 것으로 생각됩니다.

2) 기본계획의 수립과 시행에 관한 검토(안 제4조)

- 안 제4조는 교육감이 디지털재난을 효과적으로 예방·대응할 수 있도록 보안·안전체계 구축, 디지털재난 대응 매뉴얼 수립 등을 포함하는 내용의 기본계획을 매년 수립하도록 규정하고 있습니다.

아울러 동 조문은 기본계획을 「유아교육정보시스템 및 교육정보시스템의 운영 등에 관한 규칙」 제5조에⁵⁾ 따른 운영계획에 포함하여

5) 「유아교육정보시스템 및 교육정보시스템의 운영 등에 관한 규칙」 제5조(운영계획의 수립) 운영센터 및 수탁기관(이하 “운영센터등”이라 한다)의 장은 매년 1월 31일까지 다음 각 호의 사항이 포함된 정보시스템 운영계획을 수립하여 시행하여야 한다. 이 경우 수탁기관의 장은 정보시스템의 운영 및 지원업무를 위탁한 교육부장관 또는 교육감에게 정보시스템 운영계획 시행 연도의 전년도 12월 31일까지 정보시스템 운영계획을 제출하여 승인을 받아야 한다.

1. 정보시스템의 운영에 필요한 인력 및 조직에 관한 사항
2. 정보시스템 운영 및 유지보수에 관한 사항
3. 정보시스템 이용 활성화에 관한 사항
4. 정보시스템 보안 관리에 관한 사항
- 4의2. 정보시스템의 전자자료 백업 및 재해복구시스템의 구축·운영 등에 관한 사항
5. 정보시스템 사용자 교육에 관한 사항
6. 정보시스템 성능 향상에 관한 사항

수립할 수 있도록 하고 있습니다.

- 본 조문은 디지털 재난의 예방과 대응조치에 있어 관계 부서의 역할을 명확히 하고, 서울시교육청의 디지털 보안 정책의 지향을 명확하게 함으로써 관계 부서의 협업과 보안 정책의 내실화를 촉진하는 데 이바지할 수 있다고 판단됩니다.
- 다만, 서울시교육청은 기본계획 수립에 있어 「전자정부법」을 비롯한 상위법령과 「사이버안보 업무규정」 및 「국가사이버안전관리 규정」, 「보안업무규정」 등의 각종 지침이 준수될 수 있도록 세심히 계획을 수립해야 하겠습니다.

3) 안전점검 및 디지털재난 대비 훈련에 관한 검토(안 제5조)

- 안 제5조는 디지털 재난 대비를 위해 교육청 차원에서 백업시스템 등의 안전 점검을 정기적으로 시행하고, 디지털재난 대비 훈련을 시행할 수 있도록 규정하고 있습니다.
- 이 중 안 제5조제1항은 「유아교육정보시스템 및 교육정보시스템의 운영 등에 관한 규칙」 제10조에⁶⁾ 따라 구축하도록 하는 정보시스템의 백업시스템 및 재해복구시스템이 안정적으로 운영되도록 정기 점검 시행을 의무화하는 내용을 담고 있습니다.
- 이는 행정부 전산시스템의 보안 및 네트워크 장비와 무선랜, 제어 시스템 등을 대상으로 한 보안대책을 강구함에 있어 정기적인 점검과 대응을 강조하고 있는 「국가 정보보안 기본지침」의 내용을⁷⁾ 준수

7. 그 밖에 정보시스템 운영을 위하여 필요한 사항

6) 「유아교육정보시스템 및 교육정보시스템의 운영 등에 관한 규칙」 제10조(자료의 백업 등) ① 운영센터등의 장(제2조제2항에 따라 보안시스템이 구비된 별도의 장소에 서버 등 장비를 두는 경우에는 그 장소를 관리하는 기관의 장을 포함한다. 이하 같다)은 재해 또는 재난 등에 대비하기 위하여 정보시스템의 백업시스템 및 재해 복구시스템을 구축해야 한다.

7) 국가정보원의 「국가 정보보안 기본지침」은 제42조제1항을 통해 펌웨어 무결성과 운영체제 등의 버전 업데이트 등을 정기적으로 확인하는 내용을 포함하는 보안-네트워크 장비의 보안대책을 수립·시행하도록 규정하고 있고, 제53조의2 제1항을 통해 각종 설비 등을 중앙에서 감시·제어하기 위한 정보시스템의 취약점을 정기적으로 점검·제거하도록 하며, 안 제55조제4항은 관리자가 정보시스템의 로그 기록을 정기적으로 점검하여 비인가자의 접속 시도 등을

하고 있다고 생각합니다.

- 이와 함께 서울시교육청은 자체 계획인 「사이버분야 위기대응 실무 매뉴얼」을 통해 주기적인 정보보호 시스템의 정기 점검과 취약점 보완 작업 등을 추진하고 있는바, 본 조례안을 통해 디지털재난에 대비한 시스템 점검을 제도화하는 측면에서 의미가 있다고 보여집니다.
- 한편, 디지털재난 대비 훈련에 관해 다루고 있는 제5조제2항은 지방자치단체장과 공공기관장에게 매년 정기적인 사이버 위기 대응 훈련을 실시하도록 정하고 있는 「국가사이버안전관리규정」 제9조의2 제1항의8) 내용을 반영한 것으로 별도의 문제는 없을 것으로 사료됩니다.
- 다만, 서울시교육청은 안 제5조제3항에 따라 안전 점검 업무의 위탁이 이뤄지는 경우 수탁기관에 의한 자료 유출이 발생하지 않도록 관리 감독에 만전을 기해야 할 것입니다.

4) 디지털재난 고지 및 조치에 관한 검토(안 제6조)

- 안 제6조는 교육감이 디지털 재난 발생 시 발생 사실에 대하여 교육 정보시스템이나 각급 학교 누리집 등을 통해 알리고, 디지털재난으로 인해 개인정보가 유출된 때에는 「개인정보 보호법」 제34조에 따른 통지 조치 등을 수행하도록 규정하고 있습니다.
- 동 조문은 디지털 재난의 발생 사실이나 피해 수준과 같은 정보를 홈페이지 등에 공개토록 함으로써 시민의 알권리를 보장할 수 있고, 재난 상황에 대한 왜곡을 방지하여 교육 현장의 혼란을 예방할 수 있다는 점에서 매우 타당한 내용이라고 판단됩니다.
- 이와 함께 안 제6조제2항은 「개인정보 보호법」 제34조에 따른

확인하도록 규정하고 있음.

8) 「국가사이버안전관리규정」 제9조의2(사이버위기 대응 훈련) ① 중앙행정기관, 지방자치단체 및 공공기관의 장은 소관 정보통신망을 대상으로 매년 정기적으로 사이버위기 대응 훈련을 실시하여야 한다.

개인정보 유출 시 개인정보처리자의 통지·신고 의무 등을 재확인하는 내용으로 별도의 문제는 없다고 판단됩니다.

○ 참고로 서울시교육청은 동 조례안과 관련하여 별도의 의견이 없음을 밝혔습니다(행정관리담당관-4088, 2024.4.15.).⁹⁾

이상으로 「서울특별시교육청 디지털재난 대비 및 대응 조례안」에 대한 검토보고를 마치겠습니다.

의안심사지원팀장	정진국(2180-8263)	입법조사관	김지수(2180-8264)
----------	----------------	-------	----------------

9) 의원발의 조례안에 대한 검토의견서 제출(행정관리담당관-4088, 2024.4.15.)

관계 법령

재난 및 안전관리 기본법

[시행 2024. 3. 27.] [법률 제19838호, 2023. 12. 26., 일부개정]

제3조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

- “재난”이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것으로서 다음 각 목의 것을 말한다.
 - 자연재난: 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 한파, 낙뢰, 가뭄, 폭염, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 소행성·유성체 등 자연우주물체의 추락·충돌, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해
 - 사회재난: 화재·붕괴·폭발·교통사고(항공사고 및 해상사고를 포함한다)·화생방사고·환경오염사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의 피해와 국가핵심기반의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병예방법」에 따른 가축전염병의 확산, 「미세먼지 저감 및 관리에 관한 특별법」에 따른 미세먼지 등으로 인한 피해
- 다. 삭제 <2013. 8. 6.>

정보통신기반 보호법

[시행 2022. 9. 11.] [법률 제18870호, 2022. 6. 10., 일부개정]

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

- “전자적 침해행위”란 다음 각 목의 방법으로 정보통신기반시설을 공격하는 행위를 말한다.
 - 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법
 - 정상적인 보호·인증 절차를 우회하여 정보통신기반시설에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신기반시설에 설치하는 방법
- “침해사고”란 전자적 침해행위로 인하여 발생한 사태를 말한다.

개인정보 보호법

[시행 2024. 3. 15.] [법률 제19234호, 2023. 3. 14., 일부개정]

제34조(개인정보 유출 등의 통지·신고) ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 “유출등”이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

- 유출등이 된 개인정보의 항목
- 유출등이 된 시점과 그 경위
- 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
- 개인정보처리자의 대응조치 및 피해 구제절차

5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
 - ③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.
 - ④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.

유아교육법

[시행 2023. 9. 27.] [법률 제19737호, 2023. 9. 27., 일부개정]

- 제19조의2(유아교육정보시스템의 구축·운영 등) ① 교육부장관 및 교육감은 유치원 및 교육행정기관의 업무(회계관리를 포함한다)를 전자적으로 처리할 수 있도록 유아교육정보시스템(이하 “정보시스템”이라 한다)을 구축·운영하여야 한다.
- ② 교육부장관 및 교육감은 정보시스템의 운영 및 지원을 위하여 정보시스템운영센터를 설치·운영하거나 정보시스템의 효율적 운영을 위하여 필요하다고 인정하는 경우 정보시스템의 운영 및 지원 업무를 교육의 정보화를 지원하는 법인 또는 기관에 위탁할 수 있다. 이 경우 교육부장관 및 교육감은 그 위탁업무의 원활한 수행을 위하여 예산의 범위에서 보조금 및 출연금을 지급할 수 있다.
 - ③ 제1항에 따른 정보시스템의 구축·운영·접속방법 및 제2항에 따른 정보시스템운영센터의 설치·운영 등에 필요한 사항은 교육부령으로 정한다.
 - ④ 정보시스템은 「초·중등교육법」 제30조의4제1항에 따른 교육정보시스템 또는 「사회복지사업법」 제6조의2제2항에 따른 정보시스템과 연계하여 활용할 수 있다.
 - ⑤ 유치원은 회계관리 업무를 위하여 정보시스템을 사용하여야 한다.

초·중등교육법

[시행 2023. 9. 27.] [법률 제19738호, 2023. 9. 27., 일부개정]

- 제30조의4(교육정보시스템의 구축·운영 등) ① 교육부장관과 교육감은 학교와 교육행정기관의 업무를 전자적으로 처리할 수 있도록 교육정보시스템(이하 “정보시스템”이라 한다)을 구축·운영할 수 있다.
- ② 교육부장관과 교육감은 정보시스템의 운영과 지원을 위하여 정보시스템운영센터를 설치·운영하거나 정보시스템의 효율적 운영을 위하여 필요하다고 인정하면 정보시스템의 운영 및 지원업무를 교육의 정보화를 지원하는 법인이나 기관에 위탁할 수 있다. <개정 2013. 3. 23.>
 - ③ 정보시스템의 구축·운영·접속방법과 제2항에 따른 정보시스템운영센터의 설치·운영 등에 필요한 사항은 교육부령으로 정한다.