서울특별시 사이버보안에 관한 조례안에 대한 수정안

의 안 번 호	관련 3043

제안일자 : 2025. 9. 1.
제 안 자 : 주택공간위원장

1. 수정이유

○ 정의 규정에서 법령과의 정합성을 확보하고, 내부 행정적 절차 등 구체적인 사항은 규칙으로 위임함으로써 제도의 탄력적 운영을 도모함.

○ 조례에서 사용하는 표현을 보다 합리적이고 명확하게 조정하여 체계와 가독성을 개선함.

2. 수정의 주요내용

○ 용어의 정의에 법 조문을 직접 명시하면서 위계적 구조로 재정리함(안 제2조)

○ 분임사이버보안관리관의 자격요건, 업무범위와 사이버보안진단의 날 지정, 보안대책 수립 방법 등 내부 행정적 절차는 규칙으로 위임함(안 제7조, 안 제14조)

○ 자문위원회 성격과 부합하지 않는 “의결” 용어를 수정함(안 제11조)

○ 사이버보안 감사를 시장이 주도적으로 하도록 행정지침을 참고하여 시장이 별도록 정하도록 함(안 제25조)

서울특별시 사이버보안에 관한 조례안에 대한 수정안

서울특별시 사이버보안에 관한 조례안 일부를 다음과 같이 수정한다.

안 제2조제3호를 다음과 같이 하고, 같은 조 제5호를 삭제하며, 같은 조 제4호를 제5호로 하고, 같은 조에 제4호를 다음과 같이 신설한다.

3. “정보시스템”이란 「전자정부법」 제2조제13호의 정보시스템을 말한다.
4. “정보보호시스템”이란 「지능정보화 기본법」 제2조제15호에 따른 정보보호시스템을 말한다.

안 제7조제1항 후단을 다음과 같이 한다.

이 경우, 분임사이버보안관리관의 자격요건, 임명 절차 및 업무범위 등 필요한 사항은 규칙으로 정한다.

안 제7조제3항을 삭제한다.

안 제11조제5항 중 “심의·의결”을 “심의·자문”으로 하고, 같은 조 제6항 중 “출석위원 과반수의 찬성으로 의결한다”를 “회의결과는 출석위원 과반수의 찬성으로 결정한다”로 한다.

안 제14조제2항 중 “매월 세 번째 수요일을 사이버보안진단의 날로 지정·시행”을 “사이버보안진단의 날을 지정하고, 정기적으로 시행”으로 하고, 같은 조 제3항 각 호 외의 부분 중 “다음 각 호와 관련된 보안대책을 수립·이행하여야 한다”를 “보안대책을 수립·이행하여야 하며, 구체적 범위

·방법 등은 규칙으로 정한다"로 하며, 같은 항 제1호부터 제6호까지를 각각 삭제한다.

안 제25조제1항 중 "「사이버안보 업무규정」 제3조의2제1항제2호의 지침(국가 정보보안 기본지침)에 따라 각급기관등"을 "각급기관등"으로, "한다"를 "하며, 그 기준과 절차는 「사이버안보 업무규정」 제3조의2제1항제2호의 지침을 참고하여 시장이 정한다"로 한다.

수정안 조문 대비표

제 정 안	수 정 안
제2조(정의) 이 조례에서 사용하는 용어의 뜻은 다음과 같다.	제2조(정의) ----------.
1.·2. (생 략)	1.·2. (제정안과 같음)
3. “정보보호시스템”이란 정보의 수집·가공·저장·검색·송신 또는 수신 중 발생할 수 있는 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 말한다.	3. “정보시스템”이란 「전자정부법」 제2조제13호의 정보시스템을 말한다.
<신 설>	4. “정보보호시스템”이란 「지능정보화 기본법」 제2조제15호에 따른 정보보호시스템을 말한다.
4. (생 략)	5. (제정안 제4호와 같음)
5. “정보시스템”이란 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.	<삭 제>
6. (생 략)	6. (제정안과 같음)
제7조(분임사이버보안관리관 운영) ① 시장은 사이버보안관리관이 직무를 효율적으로 수행할 수 있도록 각 부서의 분임사이버보안관리관을 임명하고, 이를 보조할 분임사이버보안담당자를 지정하여야 한다. 별도로 임명하지 않은 경우 각 부서의 장을 분임사이버보안관리관으로 임명한 것으로 본다.	제7조(분임사이버보안관리관 운영) ① ----------. 이 경우, 분임사이버보안관리관의 자격요건, 임명 절차 및 업무범위 등 필요한 사항은 규칙으로 정한다.
② (생 략)	② (제정안과 같음)
③ 제6조제2항 및 제3항에 따른 사이버보안관리관은 업무를 수행하는 데에 필	<삭 제>

요한 경우 해당 업무의 일부를 분임사이버보안관리관에게 위임할 수 있다.	
제11조(위원회 구성) ① ~ ④ (생 략)	제11조(위원회 구성) ① ~ ④ (제정안과 같음)
⑤ 위원회는 안건이 발생하면 구성하고, 심의·의결 후 자동 해산한다.	⑤ ---------- - 심의·자문 ----------.
⑥ 위원회의 회의는 위원 과반수의 출석으로 개의하고 출석위원 과반수의 찬성으로 의결한다.	⑥ ---------- ---------- 회의결과는 출석위원 과반수의 찬성으로 결정한다.
⑦·⑧ (생 략)	⑦·⑧ (제정안과 같음)
제14조(사이버보안 예방 조치 등) ① (생략)	제14조(사이버보안 예방 조치 등) ① (제정안과 같음)
② 시장 및 각급기관의 장은 해당 기관의 실정에 맞게 매월 세 번째 수요일을 사이버보안진단의 날로 지정·시행하여야 한다.	② ---------- ---------- 사이버보안진단의 날을 지정하고, 정기적으로 시행---------- -------.
③ 시장 및 각급기관의 장은 정보화사업을 수행할 때에는 다음 각 호와 관련된 보안대책을 수립·이행하여야 한다.	③ ---------- ---------- 보안대책을 수립·이행하여야 하며, 구체적 범위·방법 등은 규칙으로 정한다.
1. 관리 체계 구축 및 누출금지정보의 관리 등 관리적 보안대책	<삭 제>
2. 설치·운용 장소 관리 등 물리적 보안대책	<삭 제>
3. 정보통신망, 정보시스템 등 구성 요소별 기술적 보안대책	<삭 제>
4. 긴급 사태 대비 및 재난 복구 계획	<삭 제>
5. 온라인 개발 등 용역업체 작업 장소에 대한 보안대책	<삭 제>
6. 그 밖에 규칙으로 정하는 사항	<삭 제>

④ (생 략)	④ (제정안과 같음)
제25조(사이버보안 감사) ① 시장은 「사이버안보 업무규정」 제3조의2제1항제2호의 지침(국가 정보보안 기본지침)에 따라 각급기관등의 사이버보안 업무 및 활동을 조사·점검하기 위하여 연 1회 이상 사이버보안 감사를 실시하여야 한다.	제25조(사이버보안 감사) ① ------ 각급기관등---------- ---------- ---------- ---------- ---------- 하며, 그 기준과 절차는 「사이버안보 업무규정」 제3조의2제1항제2호의 지침을 참고하여 시장이 정한다.
②·③ (생 략)	②·③ (제정안과 같음)

서울특별시조례 제　　호

서울특별시 사이버보안에 관한 조례안

제1조(목적) 이 조례는 사이버공격·위협에 체계적이고 효과적으로 대응하기 위하여 사이버보안 강화 및 관계 기관 협력 체계 강화에 필요한 사항과 「사이버안보 업무규정」에서 위임된 사항을 규정함을 목적으로 한다.

제2조(정의) 이 조례에서 사용하는 용어의 뜻은 다음과 같다.

1. “사이버공격·위협”이란 해킹, 컴퓨터 바이러스, 서비스거부, 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템 등을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 등의 행위 및 그와 관련된 위협을 말한다.
2. “각급기관”이란 서울특별시 직속기관·사업소·합의제 행정기관·의회 사무처·자치구, 「지방공기업법」에 따른 공사·공단 및 「서울특별시 출자·출연 기관의 운영에 관한 조례」에 따른 출자·출연 기관을 말한다.
3. “정보시스템”이란 「전자정부법」 제2조제13호의 정보시스템을 말한다.
4. “정보보호시스템”이란 「지능정보화 기본법」 제2조제15호에 따른 정보보호시스템을 말한다.
5. “정보통신기기등”이란 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기·설비·소프트웨어 및 정보통신서비스를 말한다.

6. “정보통신실”이란 전산실·통신실·데이터센터 등 명칭을 불문하고 서버·스위치·방화벽·침입차단시스템 등 정보시스템 및 정보보호시스템 등이 설치·운용되는 장소를 말한다.

제3조(책무) ① 서울특별시장(이하 “시장”이라 한다) 및 각급기관의 장은 사이버공격·위협으로부터 사이버공간을 보호하도록 노력하여야 한다.

② 시장 및 각급기관의 장은 서울특별시 본청 및 각급기관(이하 “각급기관등”이라 한다)의 사이버보안 업무가 원활히 수행될 수 있도록 조직, 인력 및 예산을 구성·운영하고 지도·감독하여야 한다.

③ 시장 및 각급기관의 장은 「지방자치법」 등 다른 법률에 따른 소관사무 영역을 대상으로 발생하는 사이버공격·위협으로부터 소관사무 영역을 안전하게 보호하여야 한다.

④ 각급기관의 장은 시장이 수립·시행하는 사이버보안 정책에 상응하는 사이버보안 수준 확보를 위하여 노력하여야 한다.

제4조(적용 범위) 이 조례는 서울특별시 각급기관등의 사이버보안 업무에 적용한다.

제5조(사이버보안 업무 대상 공공기관의 범위) 「사이버안보 업무규정」 제7조제2의2호에서 “조례로 정하는 기관”이란 서울특별시가 출자하거나 출연하여 설립하고 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제5조에 따라 지정·고시한 출자기관 또는 출연기관을 말한다.

제6조(사이버보안관리관 운영) ① 시장은 사이버보안 업무를 효율적이고 체계적으로 수행하고 소관사무 영역을 안전하게 보호하기 위하여 사이버보안 전문지식을 보유한 적정인력을 확보하여 사이버보안 전담 조직을 구성·운영하여야 한다.

② 시장은 다음 각 호의 업무를 전담할 사이버보안관리관을 임명하여야 한다.

1. 사이버보안 정책·계획의 수립·시행 및 사이버보안 업무의 지도·감독
2. 사이버보안 전담 조직 관리, 전문 인력의 양성
3. 정보화사업 보안성 검토 및 보안적합성 검증 업무
4. 정보통신실, 정보통신망 등의 보안 관리·감독
5. 사이버공격·위협 대응훈련 및 사이버보안 실태 점검 실시
6. 보안관제, 사고 분석·대응 및 관계 기관 정보 공유
7. 사이버보안 교육 및 사이버보안진단의 날 계획 수립·시행
8. 각급기관등에 대한 사이버보안 감사
9. 정보보호시스템의 운용, 보안 관리 및 복구 대책 수립
10. 분임사이버보안관리관 업무 감독
11. 그 밖에 규칙으로 정하는 사이버보안 관련 사항

③ 각급기관의 장은 다음 각 호의 업무를 전담할 사이버보안관리관을 임명하고, 이를 보조할 사이버보안담당자를 지정하여야 한다.

1. 소관 사이버보안 업무의 지도·감독
2. 소관 정보통신실, 정보통신망 등의 보안 관리·감독

3. 사이버공격·위협 대응훈련 및 사이버보안 실태 점검 협력

4. 보안관제, 사고 분석·대응 및 관계 기관 정보 공유 협력

5. 사이버보안 교육 및 사이버보안진단의 날 계획 수립·시행

6. 소관 정보보호시스템의 운용, 보안 관리 및 복구 대책 수립

7. 기관 분임사이버보안관리관 업무 감독

8. 그 밖에 규칙으로 정하는 사이버보안 관련 사항

④ 제3항 각 호의 업무를 수행하는 데에 필요한 경우 각급기관의 장은 시장에게 행정적·재정적 지원을 요청할 수 있다.

제7조(분임사이버보안관리관 운영) ① 시장은 사이버보안관리관이 직무를 효율적으로 수행할 수 있도록 각 부서의 분임사이버보안관리관을 임명하고, 이를 보조할 분임사이버보안담당자를 지정하여야 한다. 이 경우, 분임사이버보안관리관의 자격요건, 임명 절차 및 업무범위 등 필요한 사항은 규칙으로 정한다.

② 각급기관의 장은 각급기관의 규모와 소관 업무의 성질 등을 고려하여 사이버보안관리관 및 사이버보안담당자가 직무를 효율적으로 수행할 수 있도록 필요한 경우 각 부서의 사이버보안 업무를 수행할 수 있는 적정인력을 분임사이버보안관리관으로 임명하고, 이를 보조할 분임사이버보안담당자를 지정할 수 있다.

제8조(기본계획의 수립) 시장은 사이버보안 업무의 효율적 추진을 위하여 5년마다 다음 각 호의 사항을 포함한 서울특별시 사이버보안 기본계획(이하

“기본계획”이라 한다)을 수립·시행하여야 한다.

1. 사이버보안의 목표와 추진 방향
2. 국내외 동향, 신기술 도입 및 대응에 관한 사항
3. 사이버공격·위협 예방을 위한 대책
4. 사이버보안 교육의 활성화
5. 사이버보안 강화를 위한 전문 인력의 양성
6. 관계 기관 협력 체계 강화 방안
7. 그 밖에 규칙으로 정하는 사이버보안 강화를 위하여 필요한 사항

제9조(추진계획의 수립) ① 시장은 제8조의 기본계획에 따라 매년 사이버보안 업무에 대한 연도별 추진계획을 수립·시행하여야 한다.

② 각급기관의 장은 매년 해당 기관의 사이버보안 업무에 대한 연도별 추진계획을 수립·시행하고, 시장에게 제출하여야 한다.

제10조(사이버보안 자문위원회의 설치 및 기능) 시장은 다음 각 호의 사이버보안 업무 추진에 관한 사항을 자문하기 위하여 서울특별시 사이버보안 자문위원회(이하 “위원회”라 한다)를 설치할 수 있다.

1. 기본계획의 수립·변경
2. 주요 업무의 추진성과 평가
3. 국내외 사이버보안 환경 변화에 따른 대응 방안
4. 그 밖에 규칙으로 정하는 사항

제11조(위원회 구성) ① 위원회는 위원장 1명과 부위원장 2명을 포함하여 15명 이내로 성별을 고려하여 구성한다.

② 위원은 다음 각 호에 해당하는 사람 중에서 시장이 임명하거나 위촉하며, 위원장은 위촉직 위원 중에서 호선한다. 부위원장 2명 중 1명은 당연직 위원으로 하고 나머지 1명은 위촉직 위원 중에서 호선한다.

1. 당연직: 사이버보안 전담조직이 속한 실·본부·국의 장

2. 위촉직: 사이버보안과 관련하여 전문적인 지식이나 경험이 풍부한 사람 중 다음 각 목의 어느 하나에 해당하는 사람

가. 사이버보안 관련 전문가

나. 서울특별시 소재 기업의 정보보호 최고책임자

다. 사이버보안 전담조직이 속한 실·본부·국 소관 상임위원회 소속 의원

라. 그 밖에 규칙으로 정하는 사람

③ 위원장은 위원회를 대표하고 위원회의 업무를 총괄하며 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장(위촉직 위원을 우선한다), 위원장이 미리 지명한 위원 순으로 그 직무를 대행한다.

④ 위원회에 위원회의 사무를 처리할 간사 1명을 두며, 간사는 사이버보안 전담조직 소속 사무관이 맡는다.

⑤ 위원회는 안건이 발생하면 구성하고, 심의·자문 후 자동 해산한다.

⑥ 위원회의 회의는 위원 과반수의 출석으로 개의하고 회의결과는 출석위원 과반수의 찬성으로 결정한다.

⑦ 위원회는 이 조례 시행일부터 5년간 존속한다.

⑧ 그 밖에 위원의 위촉 해제, 제척·기피·회피, 수당 등에 관한 사항은 「서울특별시 각종 위원회의 설치·운영에 관한 조례」에 따른다.

제12조(자료 제출) 시장은 제15조에 따른 자체 진단·점검, 제19조에 따른 사고 조사, 제25조에 따른 사이버보안 감사 및 「사이버안보 업무규정」 제13조에 따른 사이버보안 실태 평가 등 사이버보안 업무의 수행에 필요한 경우 각급기관의 장에게 자료의 제출을 요청할 수 있다. 이 경우 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

제13조(사이버보안 교육) ① 시장 및 각급기관의 장은 소속 공무원(공무직 및 기간제근로자를 포함한다. 이하 같다) 및 임직원의 사이버보안에 대한 인식과 사이버보안 업무를 수행하는 소속 공무원 및 임직원의 직무역량을 높이기 위하여 필요한 교육을 연 1회 이상 실시하여야 한다.

② 소속 공무원 및 임직원은 특별한 사유가 없으면 제1항에 따른 교육을 연 1회 이상 이수하여야 한다.

③ 시장 및 각급기관의 장은 사이버보안관리관 및 사이버보안담당자의 업무 전문성을 높이고 소속 공무원의 사이버보안 지식을 함양하기 위하여 전문기관의 교육 이수나 학술회의 참가 등을 장려하여야 한다.

④ 시장은 소속 공무원의 제1항에 따른 교육의 이수 및 제3항에 따른 전문기관의 교육 이수나 학술회의 참가 등을 장려하기 위하여 행정적·재정적 지원을 할 수 있다.

제14조(사이버보안 예방 조치 등) ① 시장은 사이버공격·위협을 예방하기 위하여 각급기관등에서 시행하는 정보화사업에 대하여 보안성 검토를 실시하고, 그 검토 결과를 각급기관등에서 이행하는지를 확인할 수 있다.

② 시장 및 각급기관의 장은 해당 기관의 실정에 맞게 사이버보안진단의 날을 지정하고, 정기적으로 시행하여야 한다.

③ 시장 및 각급기관의 장은 정보화사업을 수행할 때에는 보안대책을 수립·이행하여야 하며, 구체적 범위·방법 등은 규칙으로 정한다.

④ 시장은 사이버공격·위협의 종합적 관리를 위하여 다음 각 호의 예방·대응 활동을 수행하여야 한다.

1. 정기적인 예방 점검·훈련 실시
2. 안전한 정보통신기기등의 도입 및 활용
3. 사이버공격·위협 탐지, 정보 공유, 사고 신고 등 체계의 구축·운영
4. 전문 인력 확보 및 직무교육 실시
5. 그 밖에 규칙으로 정하는 활동

제15조(사이버보안 자체 진단·점검) ① 시장은 각급기관등에 대한 사이버공격·위협을 예방하고 대응하기 위하여 다음 각 호에 대하여 연 1회 이상 자체 진단·점검을 실시하여야 한다.

1. 서버, 네트워크 장비 등 정보시스템
2. 대시민·업무용 홈페이지
3. 방화벽, 침입방지시스템 등 정보보호시스템
4. 그 밖에 규칙으로 정하는 대상

② 시장은 제1항에 따른 자체 진단·점검 이외 각급기관등의 사이버보안 강화에 필요한 경우 사이버보안 실태 점검을 실시할 수 있다.

③ 시장은 제1항에 따른 자체 진단·점검 및 제2항에 따른 사이버보안 실태 점검 결과 취약요소를 발견한 경우 각급기관의 장에게 이를 시정하는 등 필요한 조치를 요청할 수 있다. 이 경우 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

제16조(인공지능 등 신기술 활용에 대한 보안 강화) ① 각급기관등에서 다음 각 호에 해당하는 사업을 수행하고자 할 때에는 보안 위협을 사전 식별하고 보안 취약점을 제거하기 위하여 보안대책을 수립하고 시장과 협의하여야 한다.

1. 인공지능, 자율주행시스템 등 신기술 활용 사업
2. 클라우드컴퓨팅, 무선랜, 영상정보처리기기, 사물인터넷 등 내부망과 분리된 영역에 구축되어 운용되는 사업
3. 그 밖에 규칙으로 정하는 사업

② 제1항에 따른 협의에 필요한 사항은 규칙으로 정한다.

제17조(보안관제센터 설치·운영) ① 시장은 각급기관등에 대한 사이버공격·위협을 즉시 탐지·대응(이하 “보안관제”라 한다)하기 위하여 보안관제센터를 설치·운영하여야 한다.

② 보안관제센터는 다음 각 호의 업무를 수행한다.

1. 각급기관등의 정보보호시스템에서 생성된 로그의 수집 및 저장

2. 각급기관등에 대한 사이버공격·위협 탐지 및 분석

3. 각급기관등에 대한 사이버공격·위협 대응 및 초동 조치

4. 각급기관등에 대한 사이버공격·위협으로 인한 사고 조사

5. 각급기관등에 대한 사이버공격·위협에 대응하기 위한 훈련

③ 각급기관의 장은 해당 기관의 보안관제를 위하여 제1항에 따른 보안관제센터와 연계된 보안관제센터를 설치·운영하여야 한다. 다만, 해당 기관의 규모와 소관 업무의 성질 등을 고려하여 다른 기관이 운영하는 보안관제센터를 활용하는 것이 더 효율적인 경우에는 직접 설치하지 않고 다른 기관의 보안관제센터를 활용할 수 있다.

④ 시장은 제1항에 따른 보안관제를 위하여 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제4호에 따른 클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있다.

제18조(경보 발령) ① 시장 및 각급기관의 장은 「사이버안보 업무규정」 제15조에 따른 경보가 발령된 경우 경보 단계별로 사이버공격·위협에 대한 대비태세를 강화하는 등 필요한 조치를 하여야 한다.

② 경보 단계별로 시장 및 각급기관의 장이 하여야 하는 조치에 관한 사항은 규칙으로 정한다.

제19조(사고 조사·보고) ① 시장은 각급기관등에 대한 사이버공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할 수 있다.

② 시장은 제1항에 따른 사고가 발생한 경우 각급기관의 장에게 각급기관의 업무 수행 및 서비스 제공의 연속성을 확보하고 사고 영향을 최소화하는 데에 필요한 조치를 할 것을 요청할 수 있다. 이 경우 요청을 받은 각급기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

③ 각급기관의 장은 사이버공격·위협으로 사고가 발생하였음을 알게 되었을 때에는 지체 없이 그 사실을 시장에게 보고하여야 한다.

④ 시장은 사이버공격·위협으로 인한 사고로 개인정보 유출 등이 발생한 경우 그 피해를 최소화하기 위하여 각급기관등의 개인정보처리자와 적극 협력하여야 한다.

제20조(사이버보안 복구 체계) ① 시장은 제19조에 따른 사고의 피해를 최소화하기 위하여 사고의 경중에 따라 사이버보안 비상대책반을 구성·운영할 수 있다.

② 각급기관의 장은 필요시 시장에게 제1항에 따른 사이버보안 비상대책반의 구성을 요청할 수 있다.

③ 제1항에 따른 사이버보안 비상대책반 구성·운영에 필요한 사항은 규칙으로 정한다.

제21조(사이버공격·위협 대응훈련) ① 시장 및 각급기관의 장은 사이버공격·위협에 대응하기 위한 훈련을 연 1회 이상 실시하여야 한다.

② 시장은 각급기관등에 대한 사이버공격·위협에 대비한 통합 훈련을 실시할 수 있다.

③ 시장은 제2항에 따른 통합 훈련을 실시하려는 경우 특별한 사유가 없으면 사전에 훈련 일정 등을 해당 각급기관의 장에게 통보하여야 한다.

④ 시장은 제2항에 따른 통합 훈련 결과 필요하다고 판단하는 경우에는 해당 각급기관의 장에게 시정조치를 요청할 수 있다.

⑤ 제1항에 따른 훈련 및 제2항에 따른 통합 훈련의 범위와 세부 내용은 규칙으로 정한다.

제22조(위협정보의 공유) ① 시장 및 각급기관의 장은 사이버공격·위협의 예방 및 신속한 대응을 위하여 다음 각 호에 해당하는 정보(이하 “위협정보”라 한다)를 기관 간 상호 공유할 수 있다.

1. 사이버공격·위협의 방법 및 대응 조치에 관한 정보
2. 사이버공격·위협에 사용된 악성 소프트웨어 및 이와 관련된 정보
3. 정보통신망, 정보시스템, 정보보호시스템, 정보통신기기등의 보안 취약점에 관한 정보
4. 그 밖에 규칙으로 정하는 사이버공격·위협 예방 및 대응에 필요한 정보

② 시장 및 각급기관의 장은 제1항에 따라 위협정보를 공유하는 과정에서 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 한다.

제23조(협력 체계) 시장은 사이버보안 수준 향상을 도모하고 국내외 협력 체계를 강화하기 위하여 다음 각 호의 사항을 추진할 수 있다.

1. 중앙행정기관과의 사이버보안 협력 및 정보 공유를 통한 위기 대응체계 구축
2. 국제기관 및 민간기관과의 사이버보안 정보 공유 및 공동 연구
3. 제1호 및 제2호와 관련된 세미나, 콘퍼런스, 포럼 등의 개최
4. 그 밖에 협력 체계 강화를 위하여 규칙으로 정하는 사항

제24조(협의회) ① 시장은 사이버보안 정책 조정 및 정보 공유 강화를 위하여 「지방자치법」 제169조에 따른 협의회에 참여할 수 있다.

② 시장은 사이버보안 강화를 위하여 서울특별시 차원의 민·관 협력 협의회 등을 구성하거나, 필요에 따라 관계 기관이 주관하는 협의회에 참여할 수 있다.

③ 시장은 제1항 및 제2항에 따른 협의회가 원활하게 운영될 수 있도록 필요한 행정적·재정적 지원을 할 수 있다.

제25조(사이버보안 감사) ① 시장은 각급기관등의 사이버보안 업무 및 활동을 조사·점검하기 위하여 연 1회 이상 사이버보안 감사를 실시하여야 하며, 그 기준과 절차는 「사이버안보 업무규정」 제3조의2제1항제2호의 지침을 참고하여 시장이 정한다.

② 시장은 제1항에 따른 사이버보안 감사를 실시한 결과 필요한 경우 「공공감사에 관한 법률」에 따른 자체감사기구에 자체감사를 요청할 수 있다.

③ 시장은 제15조에 따라 자체 진단·점검을 실시할 때에 각급기관에서 제출한 자료를 제1항에 따른 사이버보안 감사에 활용할 수 있다.

제26조(위규자 처리) 시장은 사이버보안 위규자(규정 위반자)에 대한 처리기준을 마련·시행하여야 한다.

부 칙

제1조(시행일) 이 조례는 공포한 날부터 시행한다.

제2조(위규자 처리기준에 관한 경과조치) 이 조례 시행 전에 서울특별시 정보통신 보안업무 처리규칙에 따라 시행된 위규자(규정 위반자) 처리기준은 이 조례에 따라 시행된 것으로 본다.

제3조(임명에 관한 경과조치) 이 조례 시행 전에 서울특별시 정보통신 보안업무 처리규칙에 따라 임명된 정보보안담당관은 이 조례 제6조에 따른 사이버보안관리관에 임명된 것으로 본다.

제4조(다른 조례의 개정) 서울특별시 스마트도시 및 정보화 조례 일부를 다음과 같이 개정한다.

제21조제2항을 다음과 같이 하고, 같은 조 제3항부터 제5항까지를 각각 삭제한다.

② 그 밖에 정보보호에 관한 사항은 「서울특별시 사이버보안에 관한 조례」에 따른다.