관제 관련 업무지침

개정이력

|  |  |  |  |
| --- | --- | --- | --- |
| No. | 개정 사유 및 내용 | 개정일자 | 담당자 |
| 1 | 제정 | 2024.04.05 | 최철훈 |
|  |  |  |  |

목차

[목적 3](#_Toc128760825)

[범위 3](#_Toc128760826)

[제1조 (악성코드 보호대책) 3](#_Toc128760827)

[제2조 (성능/용량 모니터링) 4](#_Toc128760828)

[제3조 (네트워크 및 데이터흐름 모니터링) 4](#_Toc128760829)

[제4조 (장애관리) 5](#_Toc128760830)

[제5조 (침해사고 대응) 6](#_Toc128760831)

[제6조 (재해복구) 10](#_Toc128760832)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사') 소유의 자산 파괴, 정보자산의 불법적 변조나 조작, 정보자산 유출 등의 침해/재해사고 발생 또는 사고징후 포착 시 신속한 조치를 통하여 피해를 최소화하고 침해/재해사고 처리 절차를 확립함으로써 사고에 효과적으로 대처하고자 함에 그 목적이 있다.

# 범위

모든 임직원 및 회사의 모든 자산을 대상으로 한다.

# 제1조 (악성코드 보호대책)

1. (법) 정보시스템 및 개인정보처리시스템에 대한 악성코드 통제는 다음을 따른다.

가. 악성코드 예방: 백신 제품을 설치한다. 단, 리눅스/유닉스 서버에 대해서는 책임자 승인을 통해 예외로 할 수 있다.

나. 악성코드 탐지: 백신제품의 엔진을 최신화하고, 월 1회이상 검사를 수행한다. 단, 검사진행으로 인하여 운영시스템에 무리가 갈 수 있을 경우에는 검사를 예외로 할 수 있고, 서비스 및 응용 프로그램에 영향을 주지 않는 범위에서 엔진업데이트를 수행한다.

다. 악성코드 대응: 악성코드에 감염된 것으로 판단된 이후에는 원인분석 및 대응방안을 모색하기 위해 KRCERT(118)에 상담/신고 및 대응지원을 받을 수 있다.

2. (법) 업무용 단말기(PC, 노트북)에 대한 악성코드 통제는 다음을 따른다.

가. 악성코드 예방: 백신 제품을 설치한다.

나. 악성코드 탐지: 자동 업데이트 기능을 사용하거나 또는 일1회 이상 업데이트를 실시하여 최신의 상태로 유지한다.

다. 악성코드 대응: 악성코드에 감염된 것으로 판단된 이후에는 원인분석 및 대응방안을 모색하기 위해 KRCERT(118)에 상담/신고 및 대응지원을 받을 수 있다.

# 제2조 (성능/용량 모니터링)

1. 정보시스템에 대한 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 다음과 같은 기준을 기반으로 운영한다.

가. CPU: 1달 평균 90%이상의 사용률일 때 업그레이드

나. 메모리: 1달 평균 90%이상의 사용률일 때 업그레이드

다. 디스크: 1달 평균 90%이상의 사용률일 때 업그레이드

2. 정보시스템에 대한 서비스 가용성 보장을 위해, 자산 관리자는 성능 및 용량에 대한 모니터링 결과를 월1회 해당 소속의 부서장에게 보고한다. 단, 시스템을 통해 성능 및 용량을 모니터링하지 않는 경우에는 반기별로 보고한다.

3. 서비스 동시접속 가능한 최대치대비 50%이상의 동시접속이 월단위로 유지될 경우에는 스케일 업에대해 검토 후 대응을 해야한다. 단, 상장 등 단기간 접속수가 증가되는 예외상황에 대해서는 수시로 검토하여 스케일을 조정해야 한다.

# 제3조 (네트워크 및 데이터흐름 모니터링)

1. 내/외부로부터의 침해시도를 탐지할 수 있도록 정보시스템에서 발생되는 트래픽 및 이벤트로그를 수집하여야 한다.

2. 내/외부로부터의 침해시도를 탐지할 수 있는 모니터링은 다음을 따른다.

가. 대상 장비명: 정보보호시스템이나 네트워크장비

나. 검토 주기: 24\*365 실시간 모니터링

다. 보고: 해당 자산 관리자가 검토하여 그 결과를 (개인)정보보호관리자에게 보고한다.

3. (법) 정보통신망을 통해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출시도를 탐지하여야 한다. 단, 별도의 개인정보처리시스템을 이용하지 않는 업무용 단말기를 이용하여 개인정보를 처리하는 경우에는 예외로 적용하지 아니할 수 있으며 이 경우 업무용 단말기의 운영체제나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

4. 내/외부로부터의 침해시도를 탐지하기 위한 모니터링 결과 사후조치가 필요한 사항에 대해서는 사후조치를 진행하여야 한다.

# 제4조 (장애관리)

1. 정보시스템 장애 발생 시 효과적으로 대응하기 위해 다음과 같은 장애관리 절차에 따라 대응한다.

가. 탐지: 정보시스템 사용자의 신고 또는 로그검토 시

나. 분류: 장애유형 및 장애등급 분류

1) 장애유형 분류

가) H/W: CPU Faults, Memory Faults, Disk Full, Disk Faults, Power Supply 장애 등

나) System: OS hang-up, 보안관리 tool 장애, HA S/W 비정상 작동 등

다) Application: DBMS 장애, Middle ware 장애, 기타 Application 장애 등

라) 운영: 운영실수, 변경작업간 장애, DB손상, Application 조작 실수 등

마) 기타: 원인불명의 시스템 reboot 등

2) 장애등급 분류

가) A등급: 10분 이상 서비스 불가

나) B등급: 서비스는 가능하나 시스템 장애(서버, 네트웍 부분 장애)

다) C등급: 서비스는 가능하나 어플리케이션 장애(기능 부분 장애)

다. 기록: 탐지자, 탐지 일시, 탐지내용 등을 포함하여 기록을 관리

라. 분석: 해당 정보시스템 자산 관리자가 장애 원인을 분석하여 조치 방법을 마련

마. 복구: 조치 방법대로 복구 수행

바. 재발방지: 장애원인에 대한 재발방지 대책을 수립

사. 보고: 모든 등급에 대하여 정보시스템 자산 관리자가 정보시스템 자산의 책임자에게 보고

2. (법) 이용자의 가상자산에 관한 입금/출금을 정당한 사유 없이 차단하지 않도록 하여야 한다.

3. (법) .대통령령으로 정하는 정당한 사유로 이용자의 가상자산에 관한 입금/출금을 차단하는 경우, 그에 관한 사유를 미리 이용자에게 통지하고, 해당 사실을 금융위원회에 즉시 보고하여야 한다.

# 제5조 (침해사고 대응)

1. 침해사고 대응절차 내 유형별 중요도 분류, 유형별 보고 대응/복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한다.

2. 침해사고의 유형은 아래와 같다.

가. 가상자산, 월렛 개인키 등 가상자산 관련한 중요자산의 분실/도난/유출

나. 권한있는 내부자에 의한 가상자산 관련 부정거래

다. 정보자산에 대한 비인가 접근 및 의도적인 접근 시도

라. 타인의 사용자 계정 및 패스워드의 불법적인 사용

마. 자산의 불법 반출 및 의도적인 손상

바. 정보의 비인가 유출 및 도용

사. DDoS 등 정보자산의 가용성 의도적 차단

아. 침해사고 인지 후 미 보고

자. 통제구역에 비 인가된 접근 시도

차. 악성 소프트웨어(바이러스, 백도어, 트로이목마 등)의 침투

타. 기타 정보보호 관련 지침, 및 절차 등을 위반하여 업무에 영향을 미친 경우 등

3. 침해사고의 유형별 중요도 분류는 아래와 같다

가. 1등급: 가상자산 관련 중요자산(가상자산, 월렛 개인 키 등)의 분실/도난/유출/부정거래. 또는 기밀급의 데이터의 손실이나 손상으로 인해 정보시스템 및 서비스 손실을 초래하거나 잠재적으로 가능성 있는 상태

나. 2등급: 대외비급의 데이터의 손실이나 손상으로 인해 복합적으로 운영에 영향을 미치는 상태

다. 3등급: 시스템 기능성(10% 미만 사용자 영향)과 사용자에 영향을 미치는 상태

4. 유형별 보고 대응은 아래와 같다

가. 1등급: 2등급 해당 및 최고경영층까지 보고

나. 2등급: (개인)정보보호책임자

다. 3등급: (개인)정보보호관리자

5. 침해사고 복구절차는 아래와 같다

가. 1등급: 내외부 전문가를 구성하여 복구하며, 최고경영층에 결과보고

나. 2등급: 내외부 전문가를 구성하여 복구하며, (개인)정보보호책임자에게 결과보고 (최고경영층까지 추후 보고)

다. 3등급: 해당 담당자가 복구하며, (개인)정보보호관리자에게 결과보고 (최고경영층까지 추후 보고)

6. 모의 훈련을 할 수 있도록 일정, 주기, 방법, 인원 등을 포함하여 훈련 시나리오를 작성한다.

7. 침해사고를 유형 및 중요도에 따라 분류하고 분류에 따른 대응체계를 달리한다.

가. 일반적인(등급 외) 단순 장애인 경우에는 해당부서에서 처리를 한다.

나. 이외 1~3등급에 해당되는 경우 등급별에 따라 대응을 한다.

8. 침해사고의 원인 및 사고 경위에 대해 조사 및 분석하고, 그 결과를 등급별 최종보고자에게 보고한다.

9. 침해사고 내용, 발견된 취약점, 처리 사항, 재발방지대책 등을 관련조직 및 임직원들에게 공유한다

10. 침해사고를 인지한 경우 내용, 심각성, 피해정도 등과 같이 침해 등급별 유형에 따라 보고방법을 달리한다

가. 등급 외 침해사고(장애로 처리)의 경우에는 장애관리 보고체계를 따른다.

나. 유형별 중요도에 따른 침해사고의 경우에는 유형별 보고단계에 따라 보고가 이루어진다.

11. 수립된 침해사고 대응절차에 따라 신속하게 처리와 복구를 수행한다.

12. 침해사고 대응 및 복구가 완료된 이후 이를 통해 얻어진 정보를 활용하여 유사사고가 반복되지 않도록 대책을 마련한다.

13. 침해사고 관련된 재발방지 대책의 내용에 따라 필요한 경우 관련 정책, 절차, 조직 등의 대응체계를 변경하여야 한다.

14. (법) 침해사고 발생시 연락을 취할 수 있는 비상연락망에는 관련 담당자 및 외부전문가 등을 포함한다.

가. 관련업체(시스템 및 네트워크 임대업체, 보안업체, 유지보수업체 등)

나. 유관기관(KISA 등)

15. 침해사고 대응 및 처리를 신속히 수행하기 위해 각 담당자((개인)정보보호 책임자/관리자/담당자/지킴이 등)가 중심인 침해사고대응조직을 기반으로 외부 유관기관(KISA 등) 및 해당부서/업무별 담당자, 외부전문가등과의 연락 및 협조체계를 마련한다.

16. (법) 개인정보/가상자산의 분실/도난/유출 사실을 안 때에는 지체없이(72시간 이내) 다음의 모든 사항(구체적 내용이 확인되지 않았을 경우에는 확인된 내용만 우선 통지/신고 후 추가로 통지/신고)을 해당 정보주체에게 전자우편/서면/모사전송/전화/이와 유사한 방법 중 하나의. 방법으로 알려야 한다.

가. 유출 등이 된 개인정보 항목

나. 유출 등이 발생한 시점과 그 경위

다. 정보주체가 취할 수 있는 조치 (유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보)

라. 정보통신서비스 제공자 등의 대응 조치 (개인정보처리자의 대응조치 및 피해 구제절차)

마. 정보주체가 상담 등을 접수할 수 있는 부서 및 연락처

바. 정보주체에 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

17. (법) 법률 요구사항\*에 해당하는 개인정보의 분실/도난/유출이 발생된 경우 정당한 사유가 없는 한 72시간 이내에 보호위원회 또는 한국인터넷진흥원에 다음의 모든사항(구체적 내용이 확인되지 않았을 경우에는 확인된 내용만 우선 신고 후 추가로 신고)을 신고하여야 한다. [시행일: 23.9.15]

가. 유출등이 된 개인정보 항목

나. 유출등이 발생한 시점과 그 경위

다. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보

라. 개인정보처리자의 대응 조치 및 피해 구제절차

마. 정보주체가 상담/신고 등을 접수할 수 있는 부서 및 연락처

18. (법) 정보통신서비스제공자/IDC에 국한하여, 침해사고 발생 시 관계기관(한국인터넷진흥원 or 과학기술정보통신부장관)에 신고하여야 한다.

18의1. (법) 한국인터넷진흥원(또는 과학기술정보통신부장관)으로부터 "속이는 행위에 의한 정보의 수집"에 관한 정보공유를 요청받을 시, 다음의 내용이 포함된 이용약관에 따라 해당조치를 취할 수 있도록 하여야 한다.

가. "접속경로의 차단", "위반행위에 이용된 전화번호에 대한 정보통신서비스의 제공 중지" 및 "정보주체에게 위반행위에 노출되었다는 사실의 통지"에 따른 조치의 사유 및 내용

나. "위반행위에 이용된 전화번호에 대한 정보통신서비스의 제공 중지"에 따른 젱공 중지 조치의 기간

다. "접속경로의 차단", "위반행위에 이용된 전화번호에 대한 정보통신서비스의 제공 중지" 및 "정보주체에게 위반행위에 노출되었다는 사실의 통지"에 따른 조치에 대한 정보주체의 이의제기 절차

라. "접속경로의 차단", "위반행위에 이용된 전화번호에 대한 정보통신서비스의 제공 중지" 및 "정보주체에게 위반행위에 노출되었다는 사실의 통지"에 따른 조치를 한 경우 해당 조치의 사유, 내용 및 이의제기 절차 등을 정보주체에게 통지하는 방법/절차

19. 침해사고 대응절차 및 방법에 대한 효과성을 평가하기 위하여 침해사고 시나리오를 년1회 계획한 후 모의훈련을 실시한다.

20. 침해사고 훈련의 주기는 연 1회 이상으로 설정하여 실시 후 결과를 (개인)정보보호책임자에게 보고한다.

21. 침해사고 대응 모의훈련 결과 침해사고 대응체계 개선이 필요한 사항이 발견된 경우 관련된 규정을 개선하여야 한다.

\* 1천명 이상의 정보주체에 관한 개인정보가 분실/도난/유출이 된 경우, 민감정보/고유식별정보가 분실/도난/유출이 된 경우, 외부로부터의 불법적인 접근에 의해 개인정보가 분실/도난/유출이 된 경우

# 제6조 (재해복구)

1. 관리체계의 위험분석 시 핵심 서비스(업무) 및 시스템의 연속성을 위협할 수 있는 IT 재해 유형에 관한 위험분석을 실시한다.

가. CEO사망 등 업무연속성에 문제를 발생할 수 있는 유형

나. 재해 발생 시 책임자(CEO 또는 정보보호책임자) 부재에 대한 유형

다. IT서비스를 제공할 수 없는 유형 등

2. 관리체계의 위험분석 내 자산평가 시 IT재해 유형별 예상 피해규모 및 업무에 미치는 영향을 감안하여 자산평가를 진행하고, 핵심 서비스(업무) 및 시스템은 자산평가 결과로 구분한다.

3. 홍수, 지진, 화재 등으로 IT서비스에 영향을 줄 수 있는 재해 발생 시, 재해복구를 신속히 수행하기 위해 각 담당자((개인)정보보호 책임자/관리자/담당자/지킴이 등)를 중심으로 재해복구조직을 구성하여야 한다. 만약, 기 구성된 (개인)정보보호 조직이 존재한다면 이를 재해복구조직으로 갈음할 수 있다.

4. 재해발생 시 신속하게 연락을 취할 수 있도록 재해복구에 관련된 조직 내 해당부서/업무별 담당자, 유지보수업체 등의 비상연락망을 운영한다. 만약, 장애/침해 대응을 위한 비상연락망이 존재할 경우에는 이를 재해복구를 위한 비상연락망으로 갈음할 수 있다.

5. IT재해 발생 시, 단계별 복구절차(발생 시초부터 복구완료까지)는 아래와 같다

가. 재해상황 인지 및 발생 시, 비상연락망을 통하여 관련 부서 및 담당자에게 상황을 보고한다.

나. 복구 작업 중 조치사항을 기록한다.

다. 복구완료가 된 경우 원인, 조치내용 등을 분석하여 대책을 마련한다.

6. 비상대책위원장의 역할과 책임은 다음과 같다.

가. IT운영 조직 총괄책임자

나. 경보발령 및 재해선포

다. 비상사태 상황 및 결과를 최고경영자에게 보고

라. 비상대책위원장은 (개인)정보보호책임자가 겸임

7. 지원반의 역할과 책임은 다음과 같다.

가. 재해 시 모든 상황 파악 및 실무 총괄

나. 재해복구계획 수립 및 관리

다. 재해복구 모의훈련계획 수립

라. 정보보호조직((개인)정보보호 관리자/담당자 등)을 지원반으로 진행함

8. 대책반의 역할과 책임은 다음과 같다.

가. 재해 시 대응복구에 대한 실무이행(시스템, 통신, DB, 네트워크, 시설복구 등)

나. 재해복구계획 수립 시 지원

다. 재해복구 모의훈련 이행

라. 정보통신 분야와 관련된 (개인)정보보호지킴이를 대책반으로 진행하거나, IDC 등 주요장비가 외부 업체를 통해 관리될 경우에는 해당 업체담당자가 진행함

9. 재해는 다음과 같이 분류한다. 재해복구계획의 대상이 되는 재해는 대재해 및 중재해에 해당하는 경우로, 부분 및 일시적 재해, 소규모 및 부분적 장애는 장애관리의 대상이 된다.

가. 재해관리대상

1) 대재해: 정보통신실, 정보통신시스템의 작동 중단 및 복구 불가, 하드웨어/소프트웨어 및 정보통신실까지 손상 발생, 데이터통신/전원 및 보조 장비의 완전 파괴

2) 중재해: 정보통신시스템의 상당 부분이 파괴, 다수 시스템의 대체가 요구됨, 파일과 소프트웨어는 손실되지 않으며 백업이 가능함

나. 장애관리대상

1) 부분 및 일시적 장애: 시스템 장애를 일으켰으나 물리적인 손상은 없음, 일부 시스템의 대체가 요구됨, 예비 시스템 사용 가능

2) 소규모 및 부분적 장애: 하드웨어나 소프트웨어에 별다른 손상이 없으며, 전산처리가 잠시 중단되는 정도로 시스템 대체 고려

10. 대책반은 재해와 관련된 제반 수집정보를 신속하게 지원반에게 보고한다.

11. 지원반은 상황의 심각성, 시급성, 확대가능성, 파급효과, 자산 위험분석 결과 등을 통해 재해경보 단계를 평가한다.

12. 비상대책위원장은 지원반의 재해경보 단계 평가결과에 따라 재해경보 단계발령을 결정 및 선포한다.

13. 재해경보에 대한 단계는 주의단계, 경계단계, 재해단계로 구분된다.

가. 주의단계: 재해발생 가능예보를 사전에 입수하는 경우

1) 비상대책위원장: 현황점검, "주의"경보 발령

2) 지원반: 긴급 대응계획 수립, 정보수집/분석/평가 및 전파, 상황보고, 지원체계 정비 및 위기 복구 체계 정비, 신속한 전파/보고, 관련기관 및 협력사와의 협조체계 유지

3) 대책반: 일일점검, 정보통신시스템의 점검 및 보호 조치, 정보수집/분석 보고, 통신망 점검 및 보호 조치

나. 경계단계: 재해에 대한 피해 발생가능성이 높은 경우

1) 비상대책위원장: 현황 점검, "경계" 경고 발령

2) 지원반: 업무대체 및 부서 간 지원체계 확보, 백업체계 확보, 대체인력 준비, 대책반 업무분장 확인

3) 대책반: 정보통신시스템 보호강화, 대책반 가동 준비, 정보수집/분석, 신속한 보고, 대책반 산하조직 비상대기, 불요불급한 서비스 중지 등의 제한 서비스체계 준비

다. 재해단계: 재해에 대한 직접적 피해가 발생하는 경우

1) 비상대책위원장: "재해" 경보발령, 재해선포 결정

2) 지원반: 긴급 대응계획 수립, 비상대책위원장에게 위기상황 평가/결과 보고, 비상대책위원장에게 재해선포 건의, 인력 및 물자 지원

3) 대책반: 대책반 현장 투입, 재해복구센터 가동

14. IT재해 등급별 복구전략 및 대책은 아래와 같이 정의한다.

가. 3등급(L): 최고경영자에게 인지 즉시 및 대응 완료 후 보고

나. 2등급(M): 최고경영자에게 인지 즉시 및 대응 완료 후 보고

다. 1등급(H): 최고경영자에게 인지 즉시 및 대응 완료 후 보고

15. IT재해 등급별 복구목표시간 및 복구시점을 아래와 같이 자산평가 결과(H, M, L)에 따라 정의한다.

가. 3등급(L): 재해시점기준 6개월 이전부터의 정보를 3개월 이내 일부 복구해야 되는 IT재해

나. 2등급(M): 재해시점기준 6개월 이전부터의 정보를 1개월 이내 일부 복구해야 되는 IT재해

다. 1등급(H): 재해시점기준 1개월 이전부터의 정보를 7일 이내 모두 복구해야 되는 IT재해

16. IT서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한지 시험계획(시나리오, 일정, 방법, 절차 등)을 계획한 후 시험을 실시한다.

17. IT재해복구 시험주기는 연 1회 이상으로 설정하여 실시 후 결과를 (개인)정보보호책임자에게 보고한다.

18. IT재해복구 시험결과 IT환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완한다.