| | 보안사고대응관리지침 | 규정번호 | 8-0-4 | | |
|---|---|---|---|---|---|
| | | 제정일자 | 2013.03.01 | | |
| | | 개정일자 | | | |
| | | 개정번호 | Ver.0 | 총페이지 | 11 |

## 제1장 총 칙

**제1조(목적)**

이 지침은 동양미래대학교(이하 "본 대학"이라 한다) 「보안규칙」 및 「정보보안규칙」,「개인정보보호규칙」에 의거 각종 보안 사고에 대한 대응·복구 및 피해 최소화, 재발방지에 관한 사항을 규정함을 목적으로 한다.

**제2조(적용 범위)**

이 규칙은 본 대학의 전 교직원 및 본 대학을 위해 종사하는 외부업체 직원 모두에게 적용된다.

**제3조(용어정의)**

이 지침에서 사용하는 용어 정의는 다음과 같다.

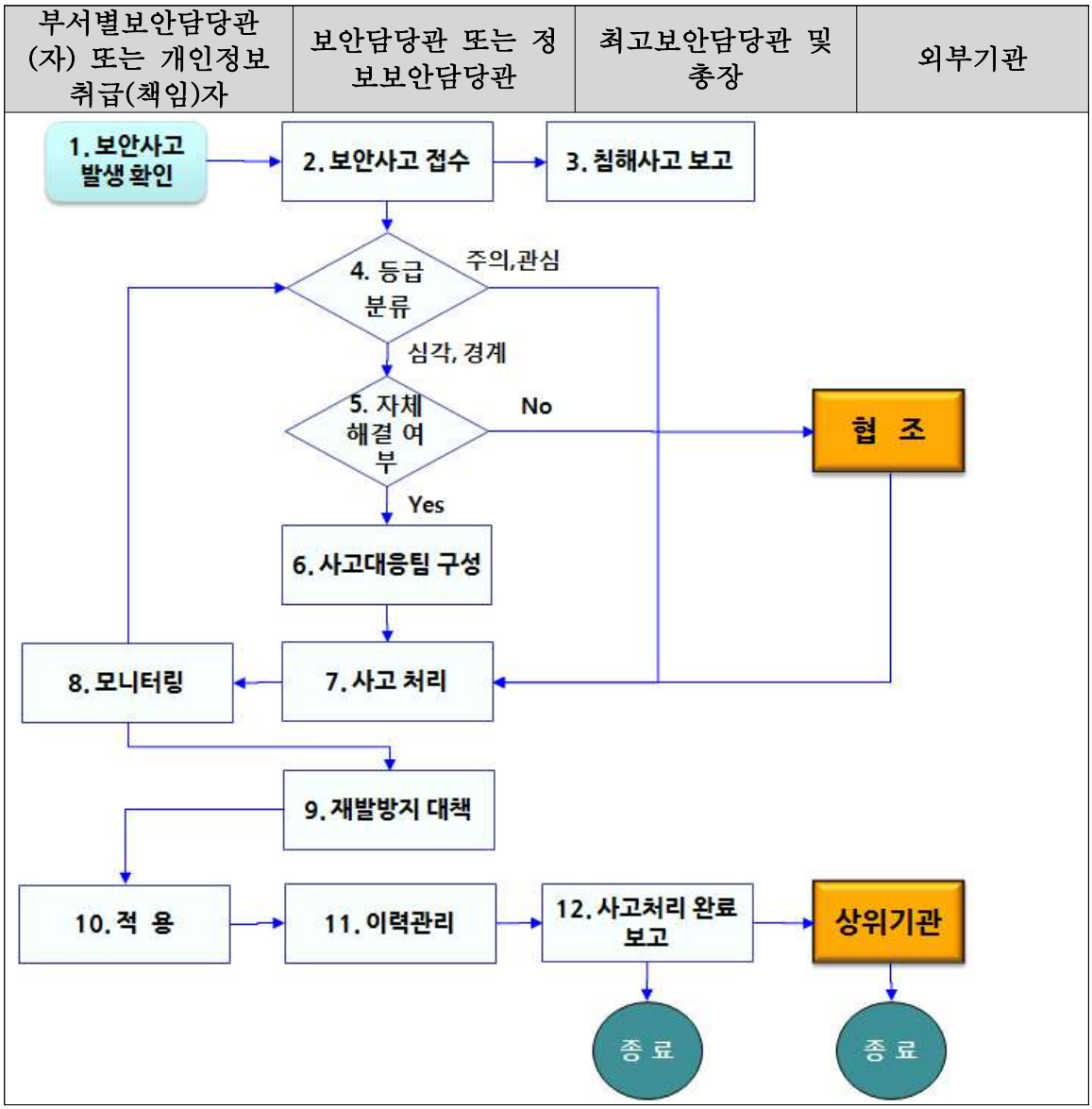
1. "보안사고"라 함은 정보통신시스템을 대상으로 관련 법·규정 등에 위배되는 사건이나 해킹, 컴퓨터 웜·바이러스, 서비스거부 등의 전자적 보안행위로 인해 본 대학의 정보자원에 손실·절도·파괴 등이 발생하여 정상적인 업무에 지장을 초래하는 사고를 말한다.
2. "공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 정보통신망을 불법 침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 사이버 공격 행위를 말한다.
3. "백도어(Backdoor)"라 함은 시스템의 보안설정을 우회할 수 있는 비밀통로로서 서비스 기술자나 유지보수개발자들의 접근 편의를 위해 고의적으로 만들어 놓은 것을 말하며, 악의적인 목적을 가진 공격자가 시스템 보안 후 해당 시스템의 재 보안을 목적으로 만들어 놓은 것을 포함한다.
4. "보안사고대응팀"이라 함은 CERT(Computer Emergency Response Team) 또는 CIRT(Computer Incident Response Team)라고도 하며, 컴퓨터 침입 사고 발생 시 신속하게 대응하기 위한 전문가들로 이루어진 그룹을 말한다.
5. 기타 용어정의는 「보안규칙」 및「정보보안규칙」,「개인정보보호규칙」등의 용어정의에 따른다.

## 제2장 보안사고 관리

**제4조(보안사고 관리 절차)**

본 대학의 보안사고 대응절차는 다음 그림과 같으며, 다음 각 호의 순서로 대응하여

야 한다.




1. 보안사고 발생 확인: 보안사고 발생 확인 즉시 사고 보고를 한다.
2. 등급분류: 보안사고의 등급은 제6조의 등급 분류표에 의한다. 주의, 관심등급은 바로 사고처리하고 심각, 경계 등급은 자체 해결 가능 여부를 판단한다.
3. 대응팀 구성: 자체 사고대응팀을 구성하여 사고대응 처리를 한다. 다만, 자체 해결이 불가능하면 외부의 침해사고대응기관에 협조를 구한다.
4. 대응전략 체계화: 최적의 전략을 결정하고 최고보안담당관의 승인을 획득하여 초기 조사결과를 참고하여 소송이 필요한 사항인지를 결정 후 조사과정에서 수사기관 공조여부를 판단한다.
5. 모니터링 및 재발방지 대책: 데이터 수집 및 분석을 통하여 수행. 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정한다.
6. 적용 및 사고처리 완료보고: 최고보안담당관은 총장이 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서를 작성하여 보고하여야 한다.

7. 이력관리: 차기 유사 공격을 식별 및 예방하기 위하여 보안정책의 수립, 지침변경, 사건의 기록, 장기 보안정책 수립, 기술 수정 계획수립 등을 결정한다.

**제5조(보안사고 예방)**

보안담당관 또는 정보보안담당관은 해킹 등 보안 사고에 대처할 수 있도록 대응방안 마련을 위하여 다음 각 호의 사항을 조치하여야 한다.

1. 불필요한 계정이나 패스워드가 없는 계정에 대한 조치를 취한다.
2. 보안 진단도구를 이용하여 시스템을 수시로 점검한다.
3. 접근통제 시스템을 구축하여 불법 침입자의 접근을 차단한다.
4. 최근의 해킹방법 및 대처방안에 대한 자료를 입수하여 대비한다.
5. 침입자 탐지시스템을 설치하여 실시간으로 침입을 식별한다.
6. 바이러스 백신 프로그램 배포 및 바이러스 정보 게시판에 게시한다.
7. 취약점 분석 및 결과에 대한 보호대책을 이행하여야 한다.

**제6조(보안사고 등급의 심각도 판단기준)**

보안사고 심각도는 해당 정도에 따라 심각(Red), 경계(Orange), 주의(Yellow) 및 관심(Blue) 4단계로 등급을 분류한다.

| 등급 구분 | 판단기준 |
|---|---|
| 심각(Red) | • 전체 정보시스템 중 70% 이상의 시스템이 바이러스/웜/DoS 공격으로 인해 사용 불능<br>• 정전 (24시간 이상), 계획된 정전은 예외로 한다.<br>• 인터넷 회선의 장애로 인한 네트워크 24시간 이상 중단<br>• 대체 장비 및 대체 사이트 필요<br>• 본 대학 및 전산실이 있는 건물의 붕괴나 화재<br>• 홍수, 폭동, 전쟁 등으로 인한 본 대학 및 전산실 진입 불가 |
| 경계 (Orange) | • 전체 정보시스템 중 15% 이상 70% 이하의 시스템 바이러스/웜/DoS 공격으로 인해 사용 불능<br>• 정전 (1시간 이상 24시간 이하), 계획된 정전은 예외로 한다.<br>• 인터넷 회선의 장애로 인한 네트워크 1시간 이상 24시간 이하 중단 |
| 주의(Yellow) | • 전체 정보시스템 중 5% 이상 15% 이하의 시스템 바이러스/웜/DoS 공격으로 인해 사용 불능 |
| 관심(Blue) | • 정전 (10분 이상 1시간 이하), 계획된 정전은 예외로 한다.<br>• 인터넷 회선의 장애로 인한 네트워크 10분 이상 1시간 이하 중단 |

## 제3장 보안사고 대응 및 복구방안

**제7조(보안사고 대응 조직)**

① 보안사고대응팀의 조직은 보안사고 발생 시 구성되며, 조직도는 별지 제1호 '보안사고대응팀(CERT) 조직도'로 정한다.

② CERT팀장은 최고보안담당관을 말하며, 보안사고대응팀(CERT)의 조직 구성을 위한 CERT팀장의 세부 수행 업무는 다음 각 호와 같다.

1. 보안사고대응담당자 지정

2. 보안 사고에 대한 주요 안건처리 및 보고
3. 유관기관에 대한 협조 요청
4. 전문가 자문 요청
5. 보안사고 대응, 비상연락망 관리
6. 기타 보안사고 대응에 필요한 사항

③ 최고보안담당관은 보안사고 접수 시, 보안사고 피해를 최소화하기 위하여 보안사고대응팀(CERT : Computer Emergency Response Team)을 구성하고, 소집하는 절차는 다음 각 호와 같다.

1. 보안사고의 효과적 대응을 위해 보안사고대응팀(이하 "CERT"라 한다)을 구성한다.
2. CERT팀장이 관련 보안사고 유형(정보보안부문, 일반 보안부문, 개인정보부문)별로 수행하여야 하는 사항은 다음 각 목과 같다.

가. 일반보안 및 개인정보 관련 사고 : 사고대응실무책임자(보안담당관)와 보안사고대응담당자 지정

나. 정보보안 사고 : 사고대응실무책임자(정보보안담당관)와 보안사고대응담당자 지정

다. 정보보안 사고 시 증거조사를 위해 외부기관 전문가의 지원 요청

3. CERT팀장은 보안사고대응담당자를 지정하여 보안사고 대응 및 보고 업무를 수행하도록 하며, 보안사고대응담당자는 별지 제1호 서식 '비상연락망'을 유지한다.
4. CERT팀장은 보안사고의 심각도가 심각(Red) 및 경계(Orange)로 판단한 시점에 CERT팀의 소집을 요청하고 CERT팀원은 소집요청에 응하여야 한다.

**제8조(보안사고 보고체계)**

① 보안사고 발생 시 '보안사고 대응절차'에 따라 단계적으로 보고하며, 보안사고 조치 완료 후에는 별지 제2호 서식 '보안사고 처리결과서'를 작성하여 최고보안담당관에게 보고한다.

② 보안사고의 보고절차는 다음과 같다.

1. 각 부서(팀) 및 학부(과) → 부서별보안담당관 경유 → 보안담당관 또는 정보보안담당관 → 최고보안담당관
2. 최고보안담당관 → 총장 → 관계 기관장

③ 최고보안담당관은 사고의 심각도에 따라 심각(Red)일 경우 CERT팀에서 결정된 사항을 총장에게 보고할 책임을 갖는다.

④ 심각도별 보안사고 보고 주기 및 형태는 아래와 같이 관련 서식 별지 제2호 서식 '보안사고 처리결과서'를 작성하여 보고한다.

| 심각도 | CERT 구성여부 | 보고자 | 결재자 | 보고 주기 | 보고 형태 |
|---|---|---|---|---|---|
| 심각(Red) | 구성 | 최고보안담당관 | 총장 | 최초보고 | 유/무선, 메일 |
| | | | | 결과보고 | 결과보고서 |
| 경계(Orange) | 구성 | 보안담당관, 정보보안담당관 | 최고보안담당관 | 최초보고 | 유/무선, 메일 |
| | | | | 결과보고 | 결과보고서 |
| 주의(Yellow) | 비구성 | 보안시스템관리자 | 보안담당관, 정보보안담당관 | 결과보고 | 유/무선, 메일 |
| 관심(Blue) | 비구성 | 보안시스템관리자 | 정보보안담당관 | 결과보고 | 유/무선, 메일 |

**제9조(보안사고대응 처리방안)**

① 시스템에 침입자 접속 시

1. 해킹 침입으로 판단될 시 '보안사고 대응절차'에 따라 단계적으로 즉시 보고한다.
2. 내부 단말기에서 침투한 경우 현재의 단말 위치를 확인한다.
3. 현재 침입자가 시스템에 있다면, 각종 도구나 명령어를 이용하여 침입자에 관련된 정보를 수집한다.
4. 침입자가 수행하고 있는 명령어를 문서로 저장하거나 기록한다.
5. 침입자가 중요한 데이터에 접근을 할 경우나 침입자를 추적할 수 없을 경우 침입자의 연결을 강제 종료 시킨다.

② 침입 흔적이 있는 경우 또는 침입자가 발견된 경우는 보안 진단도구나 체크리스트를 이용하여 다음 각 호의 사항을 점검하고 별지 제2호 서식 '보안사고 처리결과서'를 작성하여 보고하여야 한다.

1. 피해상황을 파악하여 '보안사고 대응절차'에 따라 단계적으로 즉시 보고한다.
2. 새로운 계정이 만들어져 있는지를 확인한다.
3. 패스워드 파일이 변경되었거나 모드가 변경되었는지를 확인한다.
4. 변조된 파일이 있는지 또는 외부에서 허가 없이 접속 가능한 파일들의 변경 유무를 확인한다.
5. 특정파일의 접근모드가 변경되었는지 확인한다.
6. 시스템 유틸리티의 변경 및 수정여부를 확인한다.
7. 데이터의 변조나 불법 접근의 흔적이 있을 경우 해당 서비스를 중지시킨다.
8. 침입자를 식별하기 위한 증거 수집을 한다.

**제10조(증거자료 수집, 보관)**

사고가 탐지된 경우는 모든 증거가 법정에서 사용될 것으로 예상하고 시스템 이벤트, 접속기록 등 모든 관련 로그들을 수집, 별도 보관한다.

**제11조(보안사고 처리 및 재발방지)**

① 심각도가 심각(Red) 및 경계(Orange)일 경우에 CERT팀 보안사고대응담당자는 사고경위를 조사, 분석하여야 한다.

② 사고 분석 후, 동일한 사고가 발생되지 않도록 필요한 조치에 대한 계획을 수립·

시행 하여야 하며, 사고 내용은 경위에 대한 조사가 종결될 때까지 공개하지 않는다.
③ 보안사고의 내용은 관련 조직 내에서만 공유되어야 하며, 보안사고의 재발방지에 노력하여야 한다.

## 제4장 보안사고 사후대응

**제12조(대응전략 수립)**
① 대응전략 수립단계의 목표는 주어진 사건의 환경에서 가장 적절한 대응전략을 결정하여야 한다.
② 최고보안담당관은 대응전략 수립 시 정책, 기술, 법, 업무 등 사고와 관련하여 고려하여야 하는 사항은 다음 각 호와 같다.
1. 침해를 당한 컴퓨터가 얼마나 중요하고 위험한가?
2. 침해를 당하거나 도난당한 정보가 얼마나 민감한 것인가?
3. 사건이 외부에 알려졌는가?
4. 직·간접적인 공격자는 누구인가?
5. 공격자에 의해 보안된 비인가 접근의 수준은 어느 정도인가?
6. 공격자의 수준은 어느 정도인가?
7. 시스템과 사용자의 업무중단 시간은 어느 정도인가?
8. 어느 정도의 경제적 피해가 있었는가?

**제13조(정보보안사고 상세 분석)**
① 정보보안담당관은 보안사고 심각도가 주의(Yellow) 및 관심(Blue)으로 사전 판정될 경우 탐지 및 접수된 이상 징후를 분석한다.
② 보안사고 심각도가 심각(Red) 및 경계(Orange)의 경우에는 정보보안담당관의 통제로 분석을 하되 내부 인원으로 이상 징후의 판단이 어려울 경우 외부 전문가의 지원을 받을 수 있도록 CERT팀장에게 요청할 수 있다.
③ 보안사고가 아닌 운영상의 장애 여부를 판단하기 위해 관련 부서의 협조를 요청할 수 있다.
④ 정보보안담당관은 피해 시스템에서 분석할 사항은 다음 각 호와 같다.
1. 시스템 로그 파일
2. 주요 서비스 로그 파일 (예: 웹 서버 로그, 메일서버 로그)
3. 프로세스 현황
4. 열려진 포트 현황
5. 사용자 디렉토리 점검
6. 백도어(Backdoor) 프로그램 점검 (주요 설정파일, 파일 생성시간, 파일 무결성 등)
7. 최신 해킹 프로그램 점검 등

**제14조(보고서 작성)**
① 심각도가 심각(Red) 및 경계(Orange)인 경우 사고대응실무책임자가 보안사고대응결과보고서를 작성하고 심각도가 주의(Yellow) 및 관심(Blue)인 경우 보안사고대응담

당자는 별지 제2호 서식 '보안사고 처리결과서'를 작성하여 관리하여야 한다.
② 보안사고 대응 결과 보고서에는 다음 각 호의 내용을 포함한다.
1. 보안사고 유형 및 심각도
2. 보안사고 발생 일시
3. 보안사고 대상 시스템 호스트명 및 IP
4. 보안사고 내용
5. 보안사고 발생원인
6. 보안사고 조치시간
7. 보안사고 조치 내용
8. 재발 방지를 위한 대책

**제15조(사후 대응)**
보안사고의 심각도에 따라 정보보안담당관은 재발방지 대책을 수립하여 해당 부서(팀) 및 학부(과)의 부서별보안담당관에 통보하고 해당 부서(팀) 및 학부(과)에서는 재발방지 대책을 적용하도록 하여야 한다.

**제16조(보안사고에 관한 교육 및 훈련)**
① 최고보안담당관은 재발방지를 위하여 해당 부서(팀) 및 학부(과)의 보안담당자 및 사용자를 대상으로 보안사고 발생에 대한 대응방안을 교육하여야 하며, 기록을 유지·관리하여야 한다.
② 교육 내용을 보완하여 시행할 사항은 차기 교육훈련 내용에 반영하고, 이와 관련된 정책, 절차, 조직 등 보안사고대응체계에 대해서도 교육을 수행하여야 한다.

## 부 칙

**(1) (시행일)** 이 지침은 2013년 3월 1일부터 시행한다.

[별지 제1호 서식] 비상연락망

# 비상연락망

## 1. 보안사고대응팀 연락망

| 담당업무 | 담당자 | 연락처(E-mail, HP, office) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

## 2. 관련 부서 연락망

| 부서명 | 담당자 | 담당업무 | 연락처(E-mail, HP, office) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## 3. 관련 업체 연락망

| 기관명 | 담당자 | 연락처(E-mail, HP, office) | URL |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## 4. 유관 공공기관 연락망

| 기관명 | 담당자 | 연락처(E-mail, HP, office) | URL |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

[별지 제2호 서식] 보안사고 처리결과서

# 보안사고 처리결과서

## [사고 내용]

| | | | |
|---|---|---|---|
| **사고 등급** | ☐ 심각(Red) ☐ 경계(Orange) ☐ 주의(Yellow) ☐ 관심(Blue) | **보안사고 유형** | ☐ 일반보안 ☐ 정보보안 ☐ 개인정보 |
| **사고 구분** | ☐ 침입 ☐ 장애 ☐ 취약성 ☐ 바이러스 ☐ 데이터 보안위반 ☐ 기타 | | |
| | 기타(구체적으로 기입): | | |
| **작성 일자** | | **작성 부서** | **작성자** |

| | | | |
|---|---|---|---|
| **발생 일시** | | | |
| **대상시스템 (호스트명)** | | **IP주소** | |
| **사고 내용** | | | |
| **사고 원인** | | | |

## [사고대응실무책임자 / 보안사고대응담당자 기록란]

| | | | |
|---|---|---|---|
| **조치시간** | | **조 치 자** | |
| **사고원인** | | **피해 범위** | |
| **조치내용 및 결과** | | | |
| **향후대책** | | | |

※ 작성자 : 1) 심각도가 심각(Red), 경계(Orange)인 경우 : 사고대응실무책임자

2) 심각도가 주의(Yellow), 관심(Blue)인 경우 : 보안사고대응담당자

| 결 재 | |
|---|---|
| **직위** | **서명** |
| | |
| | |
| | |
| | |

[별지 제3호 서식] 보안사고 관리대장

# 보안사고 관리대장

| 확인일자 | 확인부서 (확인자) | 시스템명 (호스트,IP) | 사고 내용 | 조치자 | 조치 결과 | 비고 (조치부서) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| 결 재 | |
|---|---|
| 직위 | 서명 |
| | |
| | |
| | |
| | |

[별지 제1호] 보안사고대응팀(CERT) 조직도