정보보안 정책

대주정공㈜

1. 개요

본 규정은 대주정공㈜(이하 '회사' 또는 '당사'라 한다.)의 정보보호 활동을 위한 기반 조직을 구성하고,비 인가자의 부적절한 행위로부터 당사 근무인원 및 시설을 안전하게 보호하는 것과 정보시스템에 의하여 처리, 저장, 소통되는 자료를 바이러스, 해킹 등의 위협으로부터 보호하고 취약요인을 제거하여 회사의 정보보호 관리를 지속적으로 이루어 지게 하는 것을 목적으로 한다

2. 적용범위

본 규정은 당사의 모든 조직과 임직원, 출입자, 전산장비 및 관련시설을 포함한 모든 정보자산에 적용한다.

3. 용어의 정의

3.1 관리적 보안 : 보안 조직 구성 및 운영, 보안정책, 절차관리, 보안교육, 보안점검, 보안감사, 보안사고조사 등의 보안활동

3.2 물리적 보안 : 비인가 자로부터 회사의 시설 및 인원을 보호하기 위한 출입통제, 정보자산의 반·출입 통제 등의 보안활동

3.3 기술적 보안 : 정보시스템의 보호 및 정보시스템을 통한 유출을 예방하기 위한 운영관리, 정보시스템 접근통제, 개발 및 유지보수, 침해사고관리 등의 보안활동

1) 정보시스템 : 사용자에게 원활한 서비스의 제공을 목적으로 하는 하드웨어 일체와 주변장치 및 운영체제를 포함한 각종 시스템 소프트웨어 및 DBMS 를 총칭한다.

2) 네트워크 : 회사의 사업을 영위하기 위해 사업장간에 송수신되는 정보 혹은 관련기관 간에 주고받는 각종 정보를 전달하여 주는 각종 시스템들을 다양한 형태로 연결시켜 주는 유무선 통신망을 의미한다.

3) 백업 : 예상치 못하고 바람직하지 않은 사건에 의해 발생할 수 있는 정보서비스 혹은 정보자산의 손상을 최소화하고 이를 복구하기 위해 필요한 복사본을 만드는 것을 말한다.

4) 복구 : 사전에 백업 받았던 복사본을 이용하여 이전의 상태로 전환하기 위한 RECOVERY 와 단순히 백업 받았던 자료를 재 설치하는 RESTORE 작업을 총칭하여 말하며, 복구를 위해서는 반드시 백업이 선행되어야 한다.

5) 단말기 : 전산시스템의 입출력 장치를 말하며, LAN 혹은 WAN 으로 연결된 개인용 PC 및 프린터, 복사기, 콘솔, 스캐너 장비 등이 포함된다

6) 정보보안사고(침해사고) : 보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출, 변조되어 정보보안관리체계에 문제가 발생하는 경우를 말한다.

7) 웹메일 : 로그인과 로그아웃의 과정을 거쳐 웹브라우저를 이용해서 메일을 보낼 수 있는 방식의 메일 서비스를 말한다.

8) VPN (Virtual Private Network) : 인터넷과 같은 공중망을 사용하여, 사설망을 구축하게 해 주는 기술 혹은 통신망의 총칭이다.

9) P2P (Peer to Peer) : 인터넷상에서 이루어지는 개인 대 개인의 파일공유 기술 및 행위를 말한다.

10) 웹하드/웹폴더 : 인터넷을 통해 모든 형태의 자료를 보관/이동/공유하거나, 파일의 보관/업로딩 및 다운로딩이 가능한 정보 저장서비스를 말한다.

11) DMZ (Demilitarized Zone) : 방화벽 구성 시 외부로 노출되어야 할 서버나 PC 등을 위해 구성된 네트워크 영역을 말한다.

12) FTP (File Transfer Protocol) : 인터넷을 통하여 어떤 한 컴퓨터에서 다른 컴퓨터로 파일을 송수신 할 수 있도록 지원하는 프로토콜을 말한다.

13) LAN (Local Area Network) : 범위가 그리 넓지 않은 일정 지역 내에서 다수의 컴퓨터나 OA 기기 등을 속도가 빠른 통신선로로 연결하여 기기간에 통신이 가능하도록 하는 근거리 통신망을 말한다.

14) IP (Internet Protocol) Address : 인터넷을 사용할 때 단말기에 할당되는 고유한 주소를 말한다.

15) 공중망 (Public Network) : 불특정 다수에게 서비스 할 수 있도록 통신업체들이 구축한 통신망으로 일반적인 사용되는 인터넷 망을 말한다.

16) 사설망 (Private Network) : 기업이나 학교 등의 특정 기관에서 사용하기 위하여 구축한 통신망을 말하며, 외부에서는 VPN 등 특정 방법을 사용하지 않는 한 접근이 되지 않는다.

4. 역할과 책임

4.1 임직원

1) 본 규정 및 관련 지침 등 보안정책을 준수 해야 한다.

2) 보안교육에 참석할 의무가 있고, 자체 점검 등 회사 보안활동에 적극 협조해야 한다.

3) 회사의 정보자산 반출 시 정해진 절차에 따라야 하며, 임의 판단으로 반출할 수 없다

4) 출입증은 항상 패용해야 하며 출입증을 타인에 대여, 공유하지 않는다

5) 보안사고를 발견하였을 경우 팀(부서)별 보안책임자 또는 보안담당조직에 즉각 해당 사실을 알려야 한다.

6) 회사의 보안규정을 위반하는 경우 다음과 같은 인원에 책임이 있다.

7) 임직원이 보안규정 위반: 위반자 및 소속 팀(부서)장

8) 방문자가 보안규정 위반: 출입허가를 요청한 임직원

4.2 방문자

1)출입증을 소속회사의 직원이나, 타인에 대여, 공유하는 행위를 해서는 안 된다.

2) 카메라 또는 카메라폰과 같은 영상 기록장치를 이용한 임의 촬영을 금지한다.

3) 당사에서 제공된 자료 외 어떤 자료도 취득, 사용해서는 안 된다.

4) 기타 당사에서 요구하는 보호조치를 준수해야 하며 위반 시 아래와 같은 책임을 진다.

5) 출입증을 대여하거나 본 목적과 다르게 사용하는 등 오.남용 적발 시 해당자의 출입증을 회수하고 출입금지 조치하며, 해당 회사에는 재발방지 대책을 요구한다.

6) 보호구역내에서는 당사의 통제를 따라야 하며 이를 위반 시 강제 퇴실 또는 퇴장된다.

7) 당사 자료를 무단으로 활용하거나 유출을 시도하는 경우에 민형사상 책임을 진다

5. 보안조직

5.1 보안조직구성 및 관리주체

1) 보안업무와 관련된 전사보안조직의 구성 및 관리는 총무기획팀에서 주관한다.

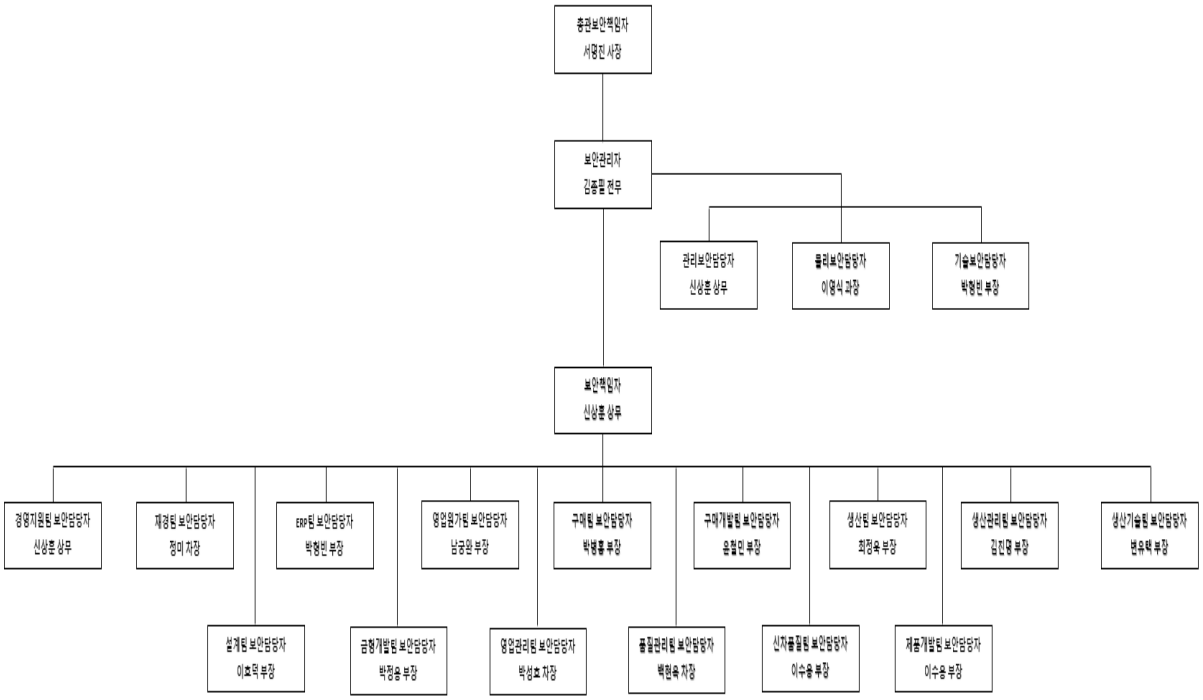
2) 보안조직 구성 및 운영에 관한 절차를 마련하고 위원의 승인을 득한 후 등록 관리한다.

3) '5.4 보안조직 업무분장'에 따로 정하지 않은 내용은 총무기획팀에서 주관한다.

5.2 보안협의체 운영

1) 보안에 대한 주요 사항의 결정 및 사내 하부조직까지의 원활한 정책 전달 및 이행을 위해 보안협의회 위원, 보안담당관, 전산보안담당자를 구성원으로 하는 협의체를 구성하고 정기적으로 운영해야 한다.

5.3 보안조직도



구분	직위	성명	임명일	비고
총괄보안책임자	사장	서명진	2023.11.30	
보안관리자	전무	김종필	2023.11.30	
관리보안담당자	상무	신상훈	2023.11.30	
물리보안담당자	과장	이영식	2023.11.30	
기술보안담당자	부장	박형빈	2023.11.30	
보안책임자	상무	신상훈	2023.11.30	
경영지원팀 보안담당자	상무	신상훈	2023.11.30	
재경팀 보안담당자	차장	정미	2023.11.30	
ERP 팀 보안담당자	부장	박형빈	2023.11.30	
영업원가팀 보안담당자	부장	남궁완	2023.11.30	
구매팀 보안담당자	부장	박병홍	2023.11.30	
구매개발팀 보안담당자	부장	윤철민	2023.11.30	
생산팀 보안담당자	부장	최정욱	2023.11.30	
생산관리팀 보안담당자	부장	김진명	2023.11.30	
생산기술팀 보안담당자	부장	변유택	2023.11.30	
설계팀 보안담당자	부장	이호덕	2023.11.30	
금형개발팀 보안담당자	부장	박정용	2023.11.30	
영업관리팀 보안담당자	차장	박성호	2023.11.30	
품질관리팀 보안담당자	차장	백현옥	2023.11.30	
신차품질팀 보안담당자	부장	이수용	2023.11.30	
제품개발팀 보안담당자	부장	이수용	2023.11.30	

5.4 보안조직 업무분장 (책임과 역할)

1) 위원장 및 위원

① 대표이사 또는 대표이사의 권한을 위임 받은 임원으로 한다.

② 보안총괄책임자로서 보안에 관련한 모든 정책을 결정한다.

③ 보안담당관을 선임한다.

④ 보안업무를 기획, 시행하도록 보안담당관에 지시하고 시행 상황을 관리감독 한다.

2) 보안담당관

① 보안담당관은 보안협의회위원이 선임한 자로 한다.

② 보안업무를 보안협의회위원에 보고, 승인 후 시행한다.

③ 회사의 보안규정을 수립하고 교육, 공지 등을 활용하여 적용한다.

④ 보안관련 법령 및 관련사의 보안정책 변경 등 외부환경 변화에 따른 회사의 보안정책을 재검토하고 필요 시 보안규정에 반영하거나 보안교육, 점검, 감사 등의 조치를 시행한다.

⑤보안의식 제고를 위해 매월 특정일을 '보안의 날'로 지정하여 자체점검을 시행한다.

⑥보안교육 및 홍보를 실시한다.

⑦보안사고 발생 시 외부 수사기관과의 연계여부를 판단하고 대책 수립 및 징계를 시행한다.

⑧정보자산의 정기적인 점검을 통해 취약성 조사 및 대응방법을 마련하여 보안사고를 사전에 예방한다.

⑨회사 정보보호실태를 분기별로 보안협의회위원 또는 위원장에게 보고한다.

⑩정보보호 활동 계획 및 예산에 대한 운영 및 승인을 시행한다.

⑪분기 1 회 이상 정기적으로 팀 보안 담당자 회의를 개최하여 보안 정책의 하부조직 전파에 노력한다.

3) 전산보안담당자

① 전산보안담당자는 물리보안, 관리보안, 기술보안 역할을 규정에서 정한 보안업무를 수행한다.

ⓐ 물리보안

- 각 팀(부서)에서 요청하는 보안구역설정을 검토, 승인하고, 그 결과를 요청부서에 회신하고 이를 현황으로 관리해야 한다.
- 물리보안시스템을 운영하며 관련된 절차를 수립하고, 그 절차에 따라 운영현황을 관리하며 필요 시 전사보안책임자담당자에 보고, 조치한다.

ⓑ 관리보안

- 교육계획을 수립 및 시행하고, 각종 보안 이벤트 시행, 모니터링, 정보자산에 대한 정기적인 점검 등을 통한 보안사고 예방활동을 수행한다.
- 보안사고 발생 시 이에 대한 조사, 조치활동을 담당한다.

ⓒ 기술보안

- 정보기술 관련한 전 부문의 보안업무를 총괄하여 수립 및 시행한다.
- 정보기술 보안운영계획 및 보안감사계획을 수립하고 시행한다.
- 정보기술 보안에 관련한 별도의 세부 지침을 마련하여 시행한다.
- 정보기술 보안시스템의 관리 및 성과분석을 실시한다.
- 전산자산의 안정적 운영 및 보안대책을 마련하고 실시한다.
- 정보기술(IT) 업무를 수행하는 자로 전사보안책임자가 지명한 직원으로 한다.
- '제 4 장 기술적보안'에 규정된 내용을 계획하고 시행한다.
- 전산자산의 취약점이 발견되면 전산담당자에게 개선을 요청해야 하며, 패치를 실시한다.
- 내·외부 전산장비에 대한 보안점검을 실시한다.

- 보안규정 상의 보안업무 수행사항을 적용 및 실행한다.
- 보안사고 발생 시 기술적인 조사, 조치 등을 지원한다.
- 위 각 호에 대한 결과를 보안담당관 또는 보안협의회위원에게 보고한다.

4) 팀(부서)보안책임자

- 각부서의 팀장이상으로 해당 부서 내 보안업무를 수행, 조정, 감독한다.
- 부서내 각종 기업비밀의 보안성 검토 및 보안문서 여부를 결정한다.
- 부서내내 자체 보안점검이 정상적으로 이행되고 있는지 확인하고 감독한다.
- 부서내 시건장치 등이 적절히 사용, 관리되고 있는지 확인하고 감독한다.
- 부서원 보안교육 실시를 주관한다.
- 부서내 보안사고 발생시 또는 발생할 우려가 있는 경우 보안담당관에게 통보한다
- 부서의 업무와 관련 있는 장소가 보안상 출입을 제한할 필요가 있는 경우 전산보안담당자에 보호구역 설정을 요청한다.
- 회사의 보안정책이 효과적으로 이행될 수 있도록 적극 지원한다.

6. 보안서약서

영업비밀의 법적인 보호와 임직원의 보안인식제고를 위해 정보보호서약서를 작성하여 제출토록 한다.

6.1 임직원

1) 임직원은 입사시 정보보안에 대한 중요성을 숙지하여 '비밀보호서약서'를 작성 후 인사담당자에게 제출해야 한다. '비밀보호서약서'는 관련 법령 및 정보의 기밀사항에 관하여 지켜야 할 사항을 명시해야 한다.

2) '비밀보호서약서'의 법적 유효성을 보장받기 위해 3 년 마다 1 회 이상 징구해야 한다.

3) 임직원은 퇴사시 본인이 보호해야 할 영업비밀의 내용과 보호기간, 부정경쟁방지 등에 관한 법령 준수 및 법적 책임 등이 포함된 '퇴직자영업비밀유지서약서'를 작성 제출해야 한다.

6.2 제 3 자(일반용역, 외주인원)

1) 일반용역을 포함한 외주인원은 계약 시 '제 3 자 보안서약서'를 작성하여 외주용역 관리부서에 제출해야 한다.

2) 계약서는 회사에서 정한 표준계약서를 사용해야 하며, 표준계약서에는 회사의 보안규정을 준수할 것과 외주인원 및 외주인원의 소속사에 보안책임이 있음을 공지하는 내용이 포함되어야 한다.

3) 기술용역 또는 기술자료 교환이 있는 계약의 경우 회사의 정보자산보호/관리를 위해 당사의 보안점검에 외주인원 소속사도 포함이 되어 있음을
고지하는 문구를 포함한 계약서를 사용해야 한다.

6.3 중요업무 수행자

1) 중요 프로젝트를 수행하는 임직원 및 외부인원은 프로젝트의 존재 사실 및 프로젝트를 수행하는 동안 알게 된 일체의 영업비밀에 대한 비밀유지를 서약하는 '프로젝트 보안서약서'를 작성해야 한다.

2) '프로젝트보안서약서'는 프로젝트명, 수행기간, 본인의 업무 등이 명기되어야 한다.

7. 보안교육

7.1 전산보안담당자

1) 전 임직원에 대해 연 1 회 이상 보안교육을 실시해야 하며 필요한 경우 대표이사의 입회를 요구할 수 있다.

2) 신입사원 입사 시 관리, 물리, 기술 각 영역에 대해 교육을 실시해야 한다.

3) 보안정책 변경 등 사유 발생 시 팀(부서)보안담당자에 공지 및 소집교육 등을 통해 교육을 실시해야 한다.

7.2 부서보안담당자

1) 내/외부 보안사고 발생 등 보안상 필요하다고 판단하는 경우 팀원에 대한 보안교육을 실시 할 수 있다.

2) 사내 규정 변경 등의 전달사항이 있는 경우 전달교육을 시행하도록 한다.

3) 팀 내 해외 주재원 근무대상자가 발생하는 경우 명령 발령일 2 주 이내에 해외 근무 시 필요한 보안조치에 대해 보안교육을 실시해야 한다.

8. 퇴직자 관리

8.1 인사담당부서

1) 퇴직자에 대해 '퇴직자정보보호서약서'를 퇴직서류에 포함하여 징구해야 한다.

2) 인사담당부서는 퇴직 후 동종업계로 전직한 사실을 인지 한경우 당사에서 취득한 영업비밀이 제공되었는지를 확인하고 위반사항을 확인하는 경우 법적 조치를 취한다.

8.2 부서보안담당자

1) 부서내 퇴직이 예정되거나, 퇴직명령이 발령된 직원에 대해 재직기간 동안 습득한 모든 영업비밀은 경우를 막론하고 대외로 유출하여서는 안되며 이를 위반할 시 '퇴직자정보보호서약서'에 의거하여 민형사상의 책임을 질 수 있다.는 내용을 공지 해야 한다.

2) 퇴직(예정)자가 해당업무 수행기간 동안 습득한 모든 영업비밀을 소속 부서에 인계하고 개인이 소지하고 있는 영업비밀은 재사용 불가한 상태로 파기하도록 요청하

고, 이를 확인해야 한다.

8.3 임직원

1) 임직원은 퇴직자가 동종업종 또는 경쟁사에 재취업하는 것을 인지하였을 경우 즉각 보안담담부서에 통보해야 한다.

8.4 기술보안담당자

1) 퇴직 명령이 발령된 후 퇴직자에 대한 출입 및 시스템상의 모든 접근 권한은 절차에 따라 모두 삭제 되어야 한다. 업무인수 인계에 따른 권한삭제 유예는 부서보안담당자의 승인에 따라 처리하며 최대 2 주를 초과할 수 없다.

9. 보안 위반자 관리

9.1 전사보안책임자

1) 위반사항의 경중을 1 차 판단하고, 경미한 위반의 경우 보안협의회위원 명의의 주의조치를 해당 직원 및 소속 부서장에 통보하며, 중요한 위반이라고 판단되는 경우 위원장에게 보고를 통해 조치 여부를 결정한다.

2) 보안 위반에 대한 징계는 취업규칙과 인사규정에 정한 징계 종류 및 절차에 따른다.

3) 유사사고 재발방지를 위한 대책을 수립, 시행하고, 임직원의 정보보호 의식을 고취시키기 위해 징계 결과는 익명을 사용하여 임직원 전원에게 공지할 수도 있다.

9.2 임직원

1) '정보보안 규정' 및 관련 지침/절차를 위반한 사실을 인지하는 경우 보안담당관 또는 전산보안담당자에 즉시 위반 사실을 통보해야 한다.

2) 본인의 실수 또는 의도하지 않게 정보가 노출, 제공되었음을 확인하는 경우 보안담당관 또는 전산보안담당자에 관련사실을 통보해야 한다.

9.3 위반자 경중 판단 기준

1) 경미한 위반

① 위반 내용이 실수 또는 과실에 의한 단순한 규칙/지침 위반이라고 인정되는 경우

② 위반이력이 없는 임직원이 규정, 절차 등의 미 인지로 규칙/지침을 위반한 경우

③ 본인의 위반사실을 통보해온 경우 중 중대한 위반에 사유가 되지 않는 경우

2) 중대한 위반

① 고의로 보안 규정, 절차, 지침을 우회하는 행위를 한 경우

② 부정한 정보취득이나, 보안사고에 관련된 사안으로 인정되는 경우

③ 중대한 과실이거나, 동일한 위반을 반복적으로 지적 받는 경우

10. 정보자산 분류

10.1 분류주체 및 주기

1) 부서보안담당자는 각 부서 단위로 분류 기준을 마련하고, 이를 바탕으로 정보의 생성자(문서작성자)가 최초분류를 시행하도록 공지, 점검 한다.

2) 임직원은 문서를 생성할 때 분류기준에 따라 등급을 구분하여 회사 보안정책이 준수되도록 분류기준을 인지하고, 항상 분류된 상태로 문서 관리 한다.

3) 부서보안담당자는 팀 내 업무 변동사항 발생 시 2 주 이내, 특별한 변동 사항이 없는 경우에도 6 개월에 1 회 정기적으로 검토/조정을 시행 한다.

4) 등급이 분류된 정보자산은 인식할 수 있는 관리자, 자산번호, 보관위치 등을 확인할 수 있는 인덱스를 부착하여 관리해야 한다.

10.2 정보자산의 구분

1) 일반자료는 대외적으로 노출, 공개되는 경우도 특별히 문제가 되지 않을 내용으로 공시자료 등 대외 공개를 목적으로 만들어 졌거나. 인터넷 검색 등을 통해 쉽게 취득할 수 있는 자료로 재 분류될 때 까지는 관리 대상에서 제외한다.

2) 대외비는 모든 임직원이 사용할 수 있으나, 외부인의 사용은 제한되는 자료로, 누설될 경우 회사에 일시적 손해를 끼치거나 해로운 결과를 초래할 우려가 있는 내용을 말한다.

3) 비밀은 누설될 경우 회사에 상당한 손실을 초래하거나 회사 사업계획의 폐기 및 수정을 초래할 우려가 있는 내용을 말한다.

4) 극비는 누설될 경우 회사의 경영상 막대한 손실을 초래하거나 회사보존을 위태롭게 할 우려가 있는 내용을 말한다.

10.3 정보자산의 관리

1) 보안담당관은 부서 단위에서 작성할 수 있는 정보자산분류기준을 제공해야 한다.

2) 보안담당관은 1 년에 1 회 이상 부서별로 파악된 정보자산의 리스트를 총괄 취합/관리하며, 파악된 자료에 대한 유효성 검증을 실시해야 한다.

11. 영업비밀관리기준

11.1 영업비밀의 정의

1) '영업비밀'이란 비밀로 유지된 생산방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말하며, 회사가 사용을 위하여 타사와의 계약관계 등을 통하여 도입한 타사의 영업비밀을 포함한다.

11.2 영업비밀의 보관 및 관리

1) 영업비밀은 생성시부터 관리를 해야 하며 중간과정의 산출물도 생성확정된 자료와

동일하게 관리되어야 한다.

2) 출력된 영업비밀은 문서등급, 출력자명, 작성 일시를 표기하고, 임의 접근이 가능하지 않은 장소에 보관하고 부서보안담당자가 지정하는 자가 관리한다.

3) 영업비밀의 보호기간은 사업계획의 지속성 및 보안문서의 효력성을 고려하여 설정해야 한다.

4) 임직원은 자리 이석 시 영업비밀이 책상 위 또는 노출된 장소에 방치되지 않도록 관리 해야 한다.

11.3 영업비밀의 이관

1) 보직 변동으로 해당 영업비밀을 소유할 필요가 없는 경우 전보자는 '업무인수인계서' 에 취급 영업비밀의 인수인계 내용을 작성하고, 전자문서 및 출력문서 등 모든 종류의 영업비밀을 인수자에 인계한다.

2) 부서별 보안책임자는 인계/ 인수 절차에 따라 영업비밀이 적절히 이관되었는지 확인하고 인계자 소유하고 있는 영업비밀이 모두 파기 되었는지 확인한다.

11.4 영업비밀의 배포 및 반출

1) 영업비밀을 언론기관, 국가기관, 협의회 및 본인의 업무와 직접적으로 관련이 없는 곳으로 반출하거나 외부의 요청으로 영업비밀을 제공해야 하는 경우 보안담당관의 사전 승인을 얻어 반출한다.

2) 1 항에 해당되지 않는 업무상 사외 반출의 경우 부서보안담당자의 승인을 얻고 회사가 정한 방법으로 반출한다. 사전 승인을 얻지 못한 경우 반출 24 시간 이내 서면으로 부서보안담당자에 사후 승인을 받아야 한다.

3) 사내 배포의 경우 영업비밀의 소유권자(작성자)의 판단에 따라 회사가 정하는 보호조치가 적용된 상태로 필요한 인원에 한정하여 배포한다.

4) 본인이 작성한 영업비밀이 아닌 경우 배포, 반출할 수 없으며, 작성자의 승인을 얻거나 작성자에 반출, 재 배포를 요청해야 한다.

11.5 영업비밀의 파기

1) 전자문서 형태의 영업비밀은 회사가 정하는 소프트웨어를 활용하여 복원 불가한 상태로 파기 해야 한다.

2) 인쇄된 영업비밀은 문서 세단기를 사용하여 원형을 확인 할 수 없는 상태로 파기 해야 한다.

12. 준거성

1) 보안담당관은 보안관련법령이 개정되거나, 고객사의 보안정책이 변경되는 경우 내부규정, 절차, 지침에 영향이 있는지 전산보안담당자를 통해 검토해야 하고 필요 시 개정해야 한다.

2) 보안담당관은 법령개정 및 고객사 정책변경 등 변경사항을 내부규정 변경사항과 함께 전 임직원이 인지할 수 있도록 공문 또는 게시판을 통하여 공지해야 하며, 필요 시 별도 교육을 실시 해야 한다.

3) 전산보안담당자는 시스템의 취약점을 주기적으로 점검하여, 내부 규정 또는 외부 법령에 위반사항이 없도록 확인하고 개선이 필요한 경우 보안담당관 보안협의회 위원, 위원장에 보고하고 조치 한다.

13. 보안점검/감사

13.1 목적

1) 회사에서 정한 보안통제가 적절히 이행되고 있는지 확인함으로써, 잠재적인 정보보안 침해의 가능성과 그로 인한 피해를 최소화 하는데 목적이 있다.

13.2 시행 주체 및 주기

1) 보안담당관의 주관 하에 사전 계획에 따라 시행하며 점검/감사를 시행할 인원은 보안담당관이 지명하고 위원의 승인을 받은 임직원으로 한다.

2) 1 년에 1 회 이상 점검/감사를 시행하며, 2 년에 1 회 이상 전 부서가 점검 대상이 되도록 계획 /시행한다.

3) 다음의 경우 상기 일정과 별도로 점검/감사를 실시할 수 있다.

① 위원 및 위원장이 필요하다고 인정할 때

② 보안사고의 발생 우려가 있을 때 보는 보안사고 발생시

13.3 점검/감사 대상

모든 인원 및 정보자산을 대상으로 한다.

1) 점검/감사 시행

① 감사 부서 및 피감사인은 점검 및 감사요청에 협조해야 한다.

② 점검 및 감사를 통해 지적된 사항은 관련 부서보안담당자에게 시정조치를 요구하며, 조치 계의 유효성 및 실제 수행여부는 보안담당관이 확인/관리해야 한다.

③ 조치결과가 부진한 경우 지속적으로 시정을 요청할 수 있으며, 감사결과가 중대한 보안규정의 위반사항으로 발견 시 인사부서의 협조를 구해 징계조치를 이행한다.

④ 보안보고서는 감사로 드러난 위험에 대한 대책방안 및 권고사항을 포함해야 하며 보안협의회 위원 및 위원장에게 보고 후 기록으로 관리 유지해야 한다.

14. 보호구역 설정

14.1 보호구역의 구분

1) 보호구역은 그 중요도에 따라 다음과 같이 제한지역, 통제구역으로 구분한다.

① 제한지역(실험실, 기관실) : 회사의 영업비밀 및 자산의 보호를 위하여 외부인의 출입을 제한하는 지역으로 회사의 모든 사무, 생산공장이 이에 해당 하며 임직원 외 외부인은 절차에 따라 승인 후 출입하도록 한다.

② 통제구역(전산실, 연구소) : 영업비밀보호를 위해 임직원의 출입을 통제할 필요가 있는 지역으로, 사진촬영 및 비 인가 임직원의 출입을 제한한다.

2) 보호구역 설정 및 표기

① 통제구역은 부서보안담당자의 의견을 수렴하여 물리보안담당자가 설정하고 전사보안책임자 및 CSO 에 보고 후 시행한다.

② 표기는 출입 시 쉽게 확인이 가능한 출입문 중앙상단 등에 부착한다. 가로 2, 세로 1 의 비율을 유지하여 가로 20cm, 세로 10cm 이상의 크기로 표기한다.

3) 보호구역의 출입관리

① 출입인가

ⓐ 임직원은 근무지역 및 제한지역의 출입이 가능하다.

ⓑ 업무상 통제구역의 출입이 필요한 경우 소속 부서장의 승인을 받아 물리보안담당자에 권한 요청을 부여 받아 출입이 가능 한다.

ⓒ 물리적보안 주관부서에서는 출입권한 요청에 대한 승인여부를 부서에 회신하고 이를 관리해야 한다.

② 출입관리

ⓐ 통제구역은 일반시설과 분리하여 설치해야 한다.

ⓑ 일반시설과 분리가 불가한 경우 보안 및 경계대책을 별도로 강구해야 한다.

ⓒ 통제구역은 외부인은 물론 임직원도 출입인가자 외는 출입을 금하며 소정의 서식에 의한 출입자명부를 비치하여 기록 유지해야 한다.

ⓓ 출입허가를 받은 외부인이 보호구역내에서 업무를 수행할 때에는 담당책임자의 통제를 따라야 하며 이를 위반 시 강제퇴실 또는 퇴장 조치한다.

ⓔ 통제구역 내에서는 일체의 면회(상담, 회의 등)을 금한다.

ⓕ 통제구역 내에서 활동은 전사보안담당자가 승인하고 임직원의 관리하에서 가능하다

15. 출입 통제

15.1 관리주체

1) 전산보안담당자는 효율적인 출입통제를 위하여 사원증에 출입기능을 부가한 출입증을 발급 패용하며 출입통제 업무를 주관한다.

15.2 출입증의 구분.

1) 임직원 출입증 : 당사의 임직원에 한해 발급되는 출입증

2) 방문증 : 당사에 출입이 필요한 협력업체에 발급되는 출입증

15.3 임직원 출입증의 발급

1) 인사명령 시 발급

① 신입사원, 중간입사자, 그룹전입 등 신규사원은 인사명령에 의거하여 물리보안담당자가 사원출입증을 발급한다.

2) 임시 방문 시 발급

① 방문의 신청은 외부인의 제한지역 내 진입이전에 등록되어야 하며 사전 통보없이 방문한 경우 내부 업무관련자의 방문신청 전까지 대기해야 한다.

② 외부인은 경비실에 신분확보에 필요한 기재사항을 기록하고 신분증을 위탁 후 방문증을 수령하여 제한지역에 출입한다.

15.4 출입증 재발급 및 권한 변경

1) 출입증 분실 시 재발급

① 출입(사원)증 분실 경위서'에 의거 5 일 이내에 사진 1 매 (3 × 4 ㎝)를 첨부하여 보안관리 부서에 재발급 의뢰한다.

2) 오손, 훼손, 파손 시 재발급

①분실 시 재발급에 준하여 재발급 신청한다.

15.5 권한 변경

1) 근무구역이 변경될 시에는 전산보안담당자에 통보하여 출입권한을 재 획득하여 변경된 사원증으로 재발급 받아야 한다.

2) 발급된 출입증의 검토

① 전산보안담당자는 발급된 출입증의 적절성 여부에 대한 주기적인 점검을 실시해야 한다.

②임직원의 업무와 부여된 출입권한의 적절성

③ 정기적으로 출입하는 외래인의 출입증 발급 기간의 적절성

④ 외래인의 출입기간 이후의 출입 여부

3) 출입증의 갱신 및 폐기

① 점검결과 분실 또는 재발급등의 사유로 보안유지가 불가하다고 판단될 때에는 재가를 득하여 즉시 폐기하고 새로이 갱신 해야 한다.

② 출입증 양식, 도안 등은 보안유지상 갱신시점에서 표시를 변경하여 발급 운용하며 별도의 품의에 의거 발급한다.

4) 출입증의 패용

① 회사 내 출입하는 당사의 직원 및 방문자는 식별이 가능하도록 출입증을 패용해야 하며 단, 생산공장은 안전상에 문제가 있는 경우 패용하지 않는다

② 경비실에 출입통제 지침을 공지하고 단속(점검)권한을 부여하며 미 패용자에 대하여는 아래와 같이 조치한다.

ⓐ 1 회 적발자: 2 회 이상 적발 시 조치사항에 대한 안내문 고지

ⓑ 2 회 적발자: 경위서 제출, 경고조치

ⓒ 3 회 적발자: 시말서 제출, 소속 팀(회사)에 경고장 발부

ⓓ 4 회 이상 적발자: 사업장 출입금지 및 사규에 의거 조치

ⓔ 경비실은 사전 통보된 방문자에 한해 소정의 신분증을 접수 받고 출입을 허가하며 방문 종료 후 경비실에 출입증과 신분증을 재 교환하여 출입을 종료한다.

5) 출입자 제한사항

① 출입증에 허가된 지역만 출입이 허용되며 권한이 없는 지역에 출입해서는 안된다.

② 임직원 및 방문자 구분 없이 출입증 미소지 시 당일 사용할 수 있는 출입증을 발급 받아 사용한다.

③ 출입증의 기술적인 장애 시 물리보안담당자에 통보 후 임시출입증을 발급 받아 출입한다.

④ 통제구역에서는 사진, 동영상 등 어떠한 형태의 촬영도 할 수 없다.

⑤ 당사의 자산은 반출증이 없는 경우 반출할 수 없다

⑥ 노트북 등 전산장비의 반·출입이 필요한 경우 해당 부서장은 보안조치계획 및 출입자 보안서약서를 작성한 후 전산보안담당자에 요청하고,

보안담당관의 허가를 득하여 반·출입한다.

6) 출입증 반납

① 퇴사 또는 직무변경에 의해 당사 근무자로 인정되지 않는 경우 사원증(출입증)을 반납해야 한다.

7) 차량 통제

① 임직원 중 사내 주차장 사용이 허가된 인원에 대해서 차량출입증을 발급하며, 차량출입증이 부착된 차량에 대해서만 출입을 허용한다.

② 방문객의 경우 사전에 차량출입을 신청하고, 전산보안담당자에 의해 승인된 차량에 대해 출입을 허용한다.

8) 배달 및 하역 제한

① 물품의 반입

ⓐ 경비실에서 내용을 확인하고 안전, 보안상 지장이 없는 물품에 한해서 반입을 허가한다.

② 택배 및 생수 배달자

ⓐ 택배는 배달원이 정문에 접수시키고 수령 자에게 이를 통보한다.

ⓑ 정문에 접수한 택배 물품에 대한 책임은 수령자가 오랫동안 찾아가지 않고 분실할 경우 물품에 대한 분실 및 오손 책임은 없다.

16. 업무연속성 관리

16.1 업무연속성 관리절차 내 보안의 반영

1) 천재지변, 화재, 폭동 등과 같은 비상사태 발생에 대비하여 전사에 걸쳐 업무연속성 계획을 개발하고 유지하기 위한 조직 및 관리 프로세스가 수립되어야 한다.

2) 비상사태 발생시 정보시스템의 계속적 운영과 업무 중단 시 최단 시간 내에 업무를 재개할 수 있도록 업무 우선순위에 따라 비상계획이 수립되고 운영
되여야 한다.

3) 업무연속성 계획의 변경 절차가 수립되어야 하며, 변경된 업무연속성 계획을 관련 임직원에게 교육하고 공지하여야 한다.

4) 업무연속성 계획은 정기적으로 테스트되고 그 유효성이 검증되어야 한다.

17. 최종사용자보안지침

17.1 목적 : 업무상 목적으로 회사에서 지급한 데스크탑 PC 및 노트북(이하 'PC'라 한다.), 프린터, 스캐너 등 개인업무용 전산장비의 정보기술보호를 위한 요구사항을 제공함에 그 목적이 있다.

17.2 관리항목

1) 개인용 전산장비 도입, 운영 및 폐기에 대한 지침이 마련되어야 한다.
2) 개인용 전산장비는 6 자리 이상의 로그인, 화면보호기 비밀번호가 설정되어 있어야 한다.
3) 모든 PC 에는 회사 업무용 목적으로 사용되는 회사에서 배포되는 프로그램만 설치가 가능하며, 불법 S/W 사용에 대한 책임은 본인에게 있다.
4) 모든 PC에는 악성코드실행방지솔루션 등 보안시스템이 설치되어야 하며, 사용자는 최신업데이트 및 최신보안패치 적용을 해야 하고, 그 현황이 유지되어야 한다.
5) PC 내의 파일을 공유할 필요가 있을 경우, 비밀번호가 설정된 공유 폴더를 설정하여, 인가된 사용자만 접근할 수 있도록 해야 한다.
6) 공용PC에 대한 관리자를 지정해야 하며, 공용PC에는 보안문서를 저장할 수 없다.
7) 인터넷을 사용하는 경우 회사의 보안정책(접근차단시스템 등)을 준수해야 하며, 승인되지 않은 인터넷망을 사용하여서는 안 된다.
8) 보안문서는 외부로 공중 네트워크(인터넷 등)를 거쳐 전송하는 것은 불허하며, 부득이한 경우는 사전 또는 사후에 관리자의 승인을 받아야 한다.
9) 사용자는 회사에서 지급한 H/W 및 S/W 의 변경을 임의로 하여서는 안되며, 이동형 저장장치는 승인절차를 거친 후 사용해야 한다.

18. 네트워크보안

18.1 목적 : 사내 네트워크 구성 및 외부 네트워크 연결 시 요구되는 정보기술보호의 수준을 향상시킴으로써 안정적인 네트워크 인프라 구축에 목적이 있다.

18.2 관리항목

1) 사내 네트워크는 외부에서 접근이 통제되는 사설망을 구축해야 한다.
2) 외부에서 공중망을 통해 내부 네트워크로 접속하고자 할 경우, 암호화 및 인증 절차를 통하여 업무상의 목적으로만 사용, 접근기록을 보관해야 한다.
3) 중요도가 높은 시스템 및 네트워크는 분리되어야 한다.
4) 허가되지 않은 전산장치의 회사 네트워크 사용을 금지한다.
5) 외부 방문객 또는 개인 노트북의 네트워크 사용 시 정보기술보안관리자의 승인을 받은 후 사용해야 한다.
6) 신규 네트워크 설치 또는 구성 변경 시 테스트 등 검증 과정을 거친 후 승인절차에 의해 설치 및 변경해야 한다.
7) 인가되지 않은 AP 는 통제되어야 하며, 무선랜은 128bit 이상의 암호화 키를 적용해야 한다.
8) 네트워크장비 설정 내용 백업 등 장애발생에 대비해야 한다.
9) 네트워크장비의 접근통제가 이루어져야 한다.

10) 네트워크의 도입, 운영, 폐기에 대한 지침이 마련되어야 한다.

19. 서버보안

19.1 목적 : 서버시스템을 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운영 관리하는데 그 목적이 있다.

19.2 관리항목

1) 서버의 도입, 운영, 폐기 프로세스에 대한 지침이 마련되어야 한다.
2) 서버시스템의 도입 및 변경은 적절한 절차에 따라 승인되어야 하며, 보안점검항목이 지정되어 있어야 한다.
3) 시스템 설치 시 기본적으로 생성되는 계정 및 사용하지 않는 계정은 삭제 및 변경되어야 하며, 적절한 계정관리를 통하여 접근 통제되어야 한다.
4) 서버시스템에 접근한 기록은 1 년 동안 보관되어야 한다.
5) 서버시스템 사용자 계정의 등록, 변경, 삭제는 공식적인 문서와 승인절차로 이루어져야 한다.
6) 모든 사용자에게는 유일한 계정을 부여해야 하며, 계정공유현황을 분석해야 한다.
7) 비밀번호는 영문, 숫자 혼합으로 6 자리 이상이며, 3 개월 이내 변경되어야 한다.
8) 서버시스템은 개발과 운영시스템이 분리되어야 한다.
9) 어플리케이션의 개발 및 변경은 적절한 절차에 따라 승인되어야 하며, 테스트 후 운영에 반영되어야 한다.
10) 테스트데이터는 사용자 정보 등 중요정보를 포함하여서는 안된다.
11) 데이터베이스에 대한 접근통제가 이루어져야 하며, 접근로그를 1 년 동안 보관해야 한다.
12) 서버시스템에 대한 주기적인 취약점 점검 및 조치가 이루어져야 한다.
13) 운영체제, 데이터베이스에 대한 백업 및 원격지 소산이 되어야 한다.
14) 서버시스템 장애에 대비한 복구계획이 마련되어야 한다.

20. 정보통신보안시스템운영

20.1 목적 : 정보통신보안시스템(침입차단시스템, 악성코드차단시스템 등)을 안정적, 효율적으로 운영 관리하기 위한 지침을 제공하는데 그 목적이 있다.

20.2 관리항목

1) 정보통신보안시스템의 도입, 운영, 폐기에 대한 지침이 마련되어야 한다.
2) 시스템은 인가된 사용자만이 접근해야 하며, 비밀번호는 영문, 숫자 혼합으로 6 자리 이상으로 설정되어야 한다.
3) 침입차단시스템은 필요한 서비스만을 명시적으로 허용하고, 그 외는 모두 불허한다.

4) FTP 와 P2P 서비스는 차단 하며, 필요 시 승인절차를 통해 허용한다.

5) 이동형 저장장치를 통제할 수 있는 시스템을 구축해야 하며, 장치별 사용현황이 분석되어야 한다.

6) 보안시스템 관리자는 로그 기능이 항상 가동되도록 하고, 주기적으로 모니터링 및 분석해야 하며, 관련 로그는 1 년 동안 보관해야 한다.

7) 분기별 1 회 이상 취약점 분석을 통한 취약점을 보완해야 한다.

21. 정보통신보안사고관리

21.1 목적 : IT 침해사고에 대한 대응 및 복구업무를 포함하고 있으며, IT 인프라에 대한 피해를 최소화하고 재발 방지를 통하여 정보자산의 보안성과 안정성을 유지하는데 필요한 지침을 제공하는데 그 목적이 있다.

21.2 관리항목

1) 정보통신보안사고 발생 시 정보기술보안관리자는 긴급히 대응하고, 그 처리 결과를 전사보안책임자 또는 대표이사에게 보고해야 한다.

2) 사내의 모든 사용자는 침해사고 발견 시 즉시 정보기술보안관리자 또는 전사보안관리자에게 보고해야 한다.

3) 외부에서 침입한 흔적이 의심되는 경우 정보기술보안관리자는 보안진단 도구나 체크리스트를 이용하여 점검해야 하며, 데이터의 변조나 불법 접근이 있을 경우 해당 서비스를 중지시킨다.

4) 침입자를 식별하기 위한 증거 수집 및 모든 기록을 유지 관리해야 한다.

5) 사안에 따라 공동작업이 필요하다고 판단될 경우 외부업체 및 대외 기관에 통보하고 협조를 요청한다.

6) 침해사고에 의한 정보시스템의 장애 시 신속히 복구되어야 하며, 장애복구에 대한 모의훈련이 주기적으로 실시되어야 한다.

7) 조치된 사안에 대해서는 근본 해결책을 강구하고, 재발방지를 위한 대응책을 마련한다.

8) 공개가 허용된 침해사고는 임직원에게 공지 또는 교육해야 한다.

22. 전산장비 반출입 관리

22.1 개요 : 전산실에 설치된 정보시스템의 안전성을 보장하기 위하여 전산실에 반입되거나 전산실로부터 반출되는 모든 장비와 물품에 대하여 적절한 통제를 통하여 관리하고, 그 내역이 포함된 기록을 유지하는 활동을 말한다.

22.2 목적 : 정보시스템 산출물 자료 및 시설장비 등의 불법유출과 위험물질의 반입

에 의한 전산자원의 장애 및 훼손, 그리고 그에 따르는 손실을 예방하기 위하여 반입 및 반출을 관리하는 것을 목적으로 한다.

22.3 업무내용

1) 반출입 관리 대상 : 전산실 반출입 관리의 대상은 다음과 같다.

▶ 전산작업 산출물(전산발행 보고서나 인쇄물 등을 포함)
▶ 정보기록매체(자기테이프, 광디스크, 디스켓, 메모리장치 등)
▶ 개인용 컴퓨터 및 노트북을 포함한 휴대용 컴퓨터
▶ 하드웨어 장비 및 부대설비나 장치
▶ 기관이나 조직의 자산으로 분류되는 물품
▶ 위험 물품, 약품
▶ 기타 비품 등

2) 반출/반입증 작성 : 반출/반입증에는 다음과 같은 내용이 기재되어야 한다.

▶ 반출/반입자에 대한 신원정보
▶ 반출/반입 대상에 대한 기재(매체, 규격, 반출주기, 내용 등)
▶ 반출처/반입처
▶ 반출입 기간 및 반출입 사유 등

3) 반출입 관리

① 반출

▶ 반출사유 발생시 해당 담당자가 반출증을 작성하여 전산실 관리 책임자의 승인을 득한다.
▶ 반출대장에 내역을 기재한다(자동화된 시스템을 사용하는 경우 등록한다).
▶ 대상물품을 반출한다.
▶ 반출을 위하여 비자격자의 통제구역 출입이 필요한 경우 출입자 관리기준에 따른다.

② 반입

▶ 반입사유가 발행하는 경우 반입증을 작성하여 전산실 관리 책임자의 승인을 득한다.
▶ 반입자원을 확인하고 반입관리대장에 기록하고 담당자가 서명한다.
▶ 대상물품을 반입한다.
▶ 반입을 위하여 비자격자의 통제구역 출입이 필요한 경우 출입자관리기준에 따른다.

23. 외주인원 보안 관리

23.1 참여인원에 대한 보안관리

① 경영지원팀은 외주업체 참여 대표와 그 인원에 대해서는 '정보누출' 금지 조항 및 개인의 친필 서명이 들어간 보안서약서를 징구하여야 한다

② 외주업체 참여인원의 보안의식 제고를 위하여 최소 연 1 회 이상 다음 각 호의 사항을 포함한 보안교육을 시행하여야 하며, 신규 및 변경인력은 사전에 보안교육을 받은 후 용역에 투입하여야 한다

③ 외주업체는 사업 수행 중 연 1 회 이상의 보안점검 또는 '누출금지 대상 정보'에 대해 외부 누출여부 확인을 시행할 수 있으며 외주업체가 이에 불응하거나, 보안점검 결과 충분히 이행되고 있지 않다고 판단될 경우 계약상대자에게 책임을 물을 수 있다.

④ 내・외부망 접근시 보안관리

a) 외주업체 사용 전산망은 방화벽 등을 활용하여 해당기관 업무망과 분리 구성하고 업무상 필요한 서버에만 제한적 접근을 허용한다.

b) 용역사업 수행시 연구소 전산망 이용이 필요한 경우 각 호에 따라 수행한다.

ㄱ) 사업 참여인원에 대한 사용자 계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 기관 내부문서 접근 금지

ㄴ) 계정별로 부여된 접속권한은 불필요시 곧바로 권한을 해지하거나 계정 폐기

ㄷ) 참여인원에게 부여한 패스워드는 정보보안담당관이 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인

ㄹ) 정보보안담당관은 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 매주 확인하여 이상유무 보고

ㅁ) 외주업체에서 사용하는 PC 는 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 ERP 팀의 보안통제 하에 제한적으로 허용한다.

ㅂ) 연구소 및 용역업체 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 방화벽 등을 이용해 원천 차단한다.

⑤ 사업완료 시 보안관리

ㄱ) 사업 완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비 이상으로 작성・관리하고 불필요한 자료는 삭제 및 폐기하여야 한다.

ㄴ) 외주업체에 제공한 자료, 장비와 중간・최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관은 금지한다.

ㄷ) 사업 완료 후 용역업체 소유 PC ・서버의 하드디스크・휴대용 저장매체 등 전자기록 저장매체는 국가정보원장이 안전성을 검증한 삭제 S/W 로 완전 삭제 후 반출하여야 한다.

ㄹ) 용역사업 관련자료 회수 및 삭제조치 후 용역업체에게 복사본 등 용역사업관련자료를 보유하고 있지 않다는 대표 명의 확약서를 징구하여야 한다.