개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
1	2017-01-22	2017-01-22	초도 제정
2			
3			
4			
5			

목 차

제 1 장 총칙

정보보안 개요

목적

본 규정은 (유)가야미(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 이루어지게 하는 것을 목적으로 한다.

적용범위

본 규정은 당사의 모든 임직원, 계약관계에 있는 자 및 출입자와 정보자산이 기록, 저장, 활용되는 모든 매체, 전산장비 및 관련시설을 포함한 모든 정보자산에 적용된다.

용어정의

관리적보안

보안 조직 구성 및 운영, 보안정책 및 절차관리, 보안교육, 보안점검, 보안사고조사 등의 보안활동을 의미한다.

1) 전사보안책임자(CSO) (Chief Security Officer)
회사의 대표로부터 정보보호에 대한 권한을 위임 받아 보안정책 수립, 교육, 점검 등 보안에 관련한 모든 업무시행 및 관리감독의 주체가 되는 임원을 의미한다.

2) 정보자산
회사가 보유하고 있는 지적 재산권과 특허, 영업 비밀 등 기술상, 경영상의 내용 그 자체와 이를 포함하고 있는 종이문서, 기록 등 출력된 문서 및 전자 문서, 전산 시스템, 소프트웨어, 영상 매체, 음원파일, 시설, 기타 유⋖무형의 모든 형태의 자산을 의미한다.

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

4) 보안문서

영업비밀 중 전산화 되어 파일로 존재하거나 출력되어 문서로 존재하는 자료로써, 외부에 유출되는 경우 회사의 경영상 기술상의 손실이 발생할 수 있는 자료를 의미한다.

5) 기밀성(Confidentiality)

정보자산이 전송, 백업, 보관 중에 허가 받지 않은 사람에게 노출되지 않아야 하는 성질

6) 무결성(Integrity)

정보자산이 파손되거나 고의로 변조되지 않고 완전하게 전송되고 보관되어야 하는 성질

7) 가용성(Availability)

장애가 발생했을 경우에도 정보자산의 이용이 지속적으로 가능하게 하는 성질

물리적보안

비인가 자로부터 회사의 시설 및 인원을 보호하기 위한 출입통제, 정보자산의 반·출입 통제, 상황모니터 등의 보안활동을 의미한다.

8) 상황모니터

사업장내 설치된 CCTV 또는 경비인력 운영을 통해 안전, 사고 및 보안현황을 실시간 확인하는 것에 관련한 활동을 의미한다.

기술적보안

정보시스템의 보호 및 정보시스템을 통한 유출을 예방하기 위한 운영관리, 정보시스템 접근통제, 개발 및 유지보수, 침해사고관리 등의 보안활동을 의미한다.

9) 정보시스템

사용자에게 원활한 서비스의 제공을 목적으로 하는 하드웨어 일체와 주변장치 및 운영체제를 포함한 각종 시스템 소프트웨어 및 DBMS를 총칭한다.

10) 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.

11) 백업

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

12) 복구

사전에 백업 받았던 복사본을 이용하여 이전의 상태로 전환하기 위한 RECOVERY와 단순히 백업 받았던 자료를 재 설치하는 RESTORE 작업을 총칭하여 말하며, 복구를 위해서는 반드시 백업이 선행되어야 한다.

13) 단말기

전산시스템의 입출력 장치를 말하며, LAN 혹은 WAN으로 연결된 개인용 PC 및 프린터, 콘솔, 스캐너 장비 등이 포함된다.

14) PC

데스크탑과 노트북을 말한다.

15) 모바일 기기

휴대폰, 스마트 폰, PDA, 태블릿 PC 등을 말한다.

16) 정보보안사고(침해사고)

보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출, 변조되어 정보보안관리체계에 문제가 발생하는 경우를 말한다.

17) 웹메일

로그인과 로그아웃의 과정을 거쳐 웹 브라우저를 이용해서 메일을 보낼 수 있는 방식의 메일 서비스를 말한다.

18) VPN (Virtual Private Network)

인터넷과 같은 공중망을 사용하여, 사설망을 구축하게 해 주는 기술 혹은 통신망의 총칭이다.

19) P2P (Peer to Peer)

인터넷상에서 이루어지는 개인 대 개인의 파일공유 기술 및 행위를 말한다.

20) 웹하드/웹폴더

인터넷을 통해 모든 형태의 자료를 보관/이동/공유하거나, 파일의 보관/업로딩 및 다운로딩이 가능한 정보 저장서비스를 말한다.

21) DMZ (Demilitarized Zone)

방화벽 구성 시 외부로 노출되어야 할 서버나 PC 등을 위해 구성된 네트워크 영역을 말한다.

22) FTP (File Transfer Protocol)

인터넷을 통하여 어떤 한 컴퓨터에서 다른 컴퓨터로 파일을 송수신 할 수 있도록 지원하는 프로토콜을 말한다.

23) LAN (Local Area Network)

범위가 그리 넓지 않은 일정 지역 내에서 다수의 컴퓨터나 OA기기 등을 속도가 빠른 통신선로로 연결하여 기기간에 통신이 가능하도록 하는 근거리 통신망을 말한다.

24) IP (Internet Protocol) Address

인터넷을 사용할 때 단말기에 할당되는 고유한 주소를 말한다.

25) 공중망 (Public Network)

불특정 다수에게 서비스 할 수 있도록 통신업체들이 구축한 통신망으로 일반적인 사용되는 인터넷 망을 말한다.

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

27) WAN(Wide Area Network)
지리적으로 멀리 떨어져 있는 넓은 지역을 연결하는 통신망을 말하며, LAN보다 속도가 느리다.

역할과 책임

임직원 및 계약관계에 있는 모든 인원

28) 본 규정 및 관련 지침에서 정하는 보안정책을 준수 해야 한다.
29) 보안교육에 참석할 의무가 있고, 자체 점검 등 회사 보안활동에 적극 협조해야 한다.
30) 영업비밀을 과도하게 취득, 보관하거나 사외로 무단 반출하는 등 보안사고의 개연성이 있는 행위를 해서는 안 된다.
31) 회사의 정보자산 반출 시 정해진 절차에 따라야 하며, 임의 판단으로 반출할 수 없다.
32) 출입증 및 업무시스템 계정은 타인에게 공유하지 않는다.
33) 보안사고를 발견하였을 경우 팀(부서)별 보안책임자 또는 보안담당조직에 즉각 해당 사실을 알려야 한다.
34) 회사의 보안규정을 위반하는 경우 다음과 같은 인원에 책임이 있다.
① 임직원이 보안규정 위반: 위반자 및 소속 팀(부서)장
② 방문자가 보안규정 위반: 출입허가를 요청한 임직원

방문자

35) 출입증을 소속회사의 직원이나, 타인에 대여, 공유하는 행위를 해서는 안 된다.
36) 카메라 또는 카메라폰과 같은 영상 기록장치를 이용한 임의 촬영을 금지한다.
37) 당사에서 공식적으로 제공된 자료 외 어떤 자료도 취득, 사용해서는 안 된다.
38) 당사에서 요구하는 보안조치 위반 시 사규와 관련법령에 따른 모든 책임을 진다.
① 출입증을 대여하거나 본 목적과 다르게 사용하는 등 오남용 적발 시 해당자는 출입증 회수 및 출입금지 조치되며, 소속사 대표이사에 재발방지 대책을 제출하도록 한다.
② 보호구역내에서는 당사의 통제에 따라야 하며 이를 위반 시 강제 퇴실 또는 퇴장된다.
③ 당사 자료를 무단으로 취득, 활용하거나 유출을 시도하는 경우: 관련 법령에 따른 민형사상 책임을 진다.

제 2 장 관리적 보안

보안조직

보안조직 구성 및 관리주체

39) 전사보안조직의 구성 및 관리는 인사담당팀(부서)에서 주관한다.

40) 인사담당팀(부서)는 보안에 대한 임직원의 역할과 책임을 정의하고 그 현황을 유지한다.

41) **'2.4 보안조직 업무분장'**에 따로 정하지 않은 내용은 보안협의체의 심의과정을 통하여 정의한다.

보안협의체 운영

42) 보안에 대한 정책 결정, 전달 및 이행을 위해 전사보안책임자(CSO), 보안책임자, 보안담당자를 구성원으로 하는 협의체를 구성하고 최소 반기 별로 운영해야 한다.

보안조직도

43) 관리보안 담당자는 담당자의 팀, 성명, 연락처를 포함한 보안 조직도(첨부 참조)를 작성하여 전사보안 책임자에게 보고 후 관리한다.

보안조직 업무분장 (책임과 역할) (1. 업무분장 기준 참조)

전사보안책임자(CSO) (보안담당임원)

44) 대표이사 또는 대표이사의 권한을 위임 받은 임원으로 한다.

45) 보안총괄책임자로서 보안에 관련한 모든 정책을 결정한다.

46) 전사보안관리자와 전사보안담당자를 선임한다.

47) 보안업무를 기획, 시행하도록 전사보안관리자에 지시하고 시행 상황을 관리감독 한다.

전사보안관리자

48) 전사보안책임자(CSO)가 선임한 자로 회사 모든 보안업무를 전사보안책임자(CSO)에 보고하고 시행한다.

49) 회사의 보안규정을 수립하고 교육, 공지 등을 활용하여 적용한다.

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

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

52) 보안교육 및 홍보를 실시한다.

53) 보안사고 발생 시 외부 수사기관과 연계하여 진행한다. 사고 처리 완료 후에는 재발 방지 대책을 수립하고, 필요한 경우 인사 주관부서에 징계처리를 요청한다.

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

55) 회사 정보보호실태를 분기별로 전사보안책임자(CSO)에게 보고한다.

56) 정보보호 활동 계획 및 예산에 대한 운영 및 승인을 시행한다.

57) 반기 1회 이상 정기적으로 팀 보안 담당자 회의를 개최하여 보안 정책의 하부조직 전파에 노력한다.

전사보안담당자

전사보안담당자는 관리보안담당자, 물리보안담당자, 기술보안담당자로 역할을 구분하고, 규정에서 정한 보안업무를 수행한다.

58) 관리보안담당자

① 교육계획을 수립 및 시행하고, 각종 보안 이벤트 시행, 모니터링, 정보자산에 대한 정기적인 점검 등을 통한 보안사고 예방활동을 수행한다.

② 보안사고 발생 시 이에 대한 관리적인 조사, 조치활동을 담당한다.

59) 물리보안담당자

① 각 팀(부서)에서 요청하는 보안구역설정을 검토, 승인하고, 그 결과를 요청부서에 회신하고 이를 현황으로 관리해야 한다.

② 물리보안시스템을 운영하며 관련된 절차를 수립하고, 그 절차에 따라 운영현황을 관리하며 필요 시 전사보안관리자에 보고, 조치한다.

60) 기술보안담당자

① 정보기술 관련한 전 부문의 보안업무를 총괄하여 수립 및 시행한다.

② 정보기술 보안운영계획을 수립하고 시행한다.

③ 정보기술 보안에 관련한 별도의 세부 지침을 마련하여 시행한다.

④ 정보기술 보안시스템의 관리 및 성과분석을 실시한다.

⑤ 전산자산의 안정적 운영 및 보안대책을 마련하고 실시한다.

⑥ 정보기술(IT) 업무를 수행하는 자로 전사보안책임자가 지명한 직원으로 한다.

⑦ '제4장 기술적 보안'에 규정된 내용을 계획하고 시행한다.

⑧ 전산자산의 취약점이 발견되면 전산담당자에게 개선을 요청해야 하며, 패치를 실시한다.

⑨ 내·외부 전산장비에 대한 보안점검을 실시한다.

⑩ 보안규정 상의 보안업무 수행사항을 적용 및 실행한다.

⑪ 보안사고 발생 시 기술적인 조사, 조치 등을 지원한다.

⑫ 위 각 호에 대한 결과를 전사보안책임자(CSO) 또는 전사보안관리자에게 보고한다.

팀(부서)별 보안책임자

각 팀의 팀(부서)장으로 해당 팀(부서)내 보안업무를 수행, 조정, 감독한다.

61) 팀(부서)내 각종 기업비밀의 보안성 검토 및 보안문서 여부를 결정한다.

62) 팀(부서)내 자체 보안점검이 정상적으로 이행되고 있는지 확인하고 감독한다.

63) 팀(부서)내 시건 장치 등이 적절히 사용, 관리되고 있는지 확인하고 감독한다.

64) 팀(부서)원 보안교육 실시를 주관한다.

65) 팀(부서)보안담당자를 임명한다.

66) 팀(부서)내 보안사고 발생시 또는 발생할 우려가 있는 경우 전사보안관리자에게 통보한다.

67) 팀(부서)의 업무와 관련 있는 장소가 보안상 출입을 제한할 필요가 있는 경우 물리보안담당자에 보호구역 설정을 요청한다.

68) 회사의 보안정책이 효과적으로 이행될 수 있도록 적극 지원한다.

팀(부서)별 보안담당자

69) 팀(부서)별 보안책임자가 임명한 자로 팀(부서)보안책임자의 권한을 대행하여 팀(부서)내 보안현황을 관리하고, 보안점검, 보안교육 등 팀(부서)과 관련한 보안활동을 수행한다.

70) 매월 보안의 날 시행 후 팀(부서)내 보안현황, 문제점 등을 팀(부서)보안책임자에 보고하고, 지시에 따라 개선을 이행한다.

71) 전사보안담당자가 소집하는 팀보안담당자 회의에 참석하여, 팀(부서) 입장을 대변하여 보안정책 결정에 참여하며, 정해진 보안정책을 팀 내 전파하는 역할을 수행한다.

보안서약서

관리주체

72) 영업비밀의 법적인 보호와 임직원의 보안인식제고를 위해 보안서약서(영업비밀보호서약서)를 작성하여 제출토록 한다.

73) 관리보안담당자는 징구 대상과 서약서 징구 현황을 표로 관리해야 하며, 누락이 있는지 정기적으로 점검하고 누락이 확인되는 경우 원인을 파악 후 전사보안책임자(CSO)에 보고, 조치 한다.

74) 임직원, 제3자 구분 없이 보안서약서를 제출한 인원만 당사 사업장 출입 및 정보자산을 사용할 수 있다.

75) 서약서를 제출하지 않은 인원에는 사업장 출입권한 및 시스템 사용권한을 부여해서는 안 되며, 이에 대한 관리 책임은 관리보안담당자에 있다.

임직원

76) 임직원은 입사시 정보보안에 대한 중요성을 숙지하여 보안서약서(영업비밀보호서약서)를 작성 후 채용담당자에게 제출해야 한다. 보안서약서는 관련 법령 및 정보의 기밀사항에 관하여 지켜야 할 사항을 명시해야 한다.

77) 경력직 인원에 대해서는 '전직장 영업비밀보호서약서'를 징구해야 한다.

78) 임원 선임 시에는 '영업비밀보호서약서(임원)'를 선임서류에 포함하여 징구해야 한다.

79) 관리보안담당자는 재직 중인 임직원을 대상으로 정기적으로 보안서약서를 징구해야 한다.

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

제3자(일반용역, 외주인원)

81) 일반용역을 포함한 외주인원은 계약 시 '제 3 자 보안서약서'를 작성하여 각 소속 사에 제출하여야 하며, 소속 사 관리담당자는 외주용역 관리부서에 제출해야 한다.

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

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

보안교육

전사보안책임자

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

85) 신입사원 및 경력사원 입사 시 관리, 물리, 기술 각 보안영역에 대한 회사의 정책과 신입사원 및 경력사원 이 알아야 할 주요 규정, 지침, 절차를 교육하고, 그 결과를 문서로 유지해야 한다.

86) 보안정책 변경 등 사유 발생 시 2주 이내에 팀(부서)보안담당자에 공지 또는 소집교육 등을 통해 보안정책이 변경되었음을 알 수 있도록 해야 한다.

87) 외부인이 상주하여 근무하는 경우, 업무 개시 전 보안사항에 대한 안내(교육)를 실시해야 한다.

팀(부서)보안책임자

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

89) 사내 규정 변경 등 전달사항이 있는 경우 팀(부서)보안담당자가 팀 내 전달교육을 시행하도록 한다.

퇴직자 관리

인사담당부서

90) 퇴직자에 대해 '퇴직자 영업비밀유지서약서'를 퇴직서류에 포함하여 징구해야 한다.

91) 퇴직자 영업비밀유지서약서를 제출하지 않는 인원에는 해당양식을 송부하여 제출을 독려해야 하며, 미제출시 정상적 퇴직절차가 지연될 수 있음을 공지한다.

92) 인사담당부서는 퇴직 후 동종업계로 전직한 사실을 인지한 경우 당사에서 취득한 영업비밀이 제공되었는지를 확인하고 전직금지 가처분 신청 등 관련 법적 조치를 취한다.

93) 퇴직자에 의한 중요정보 유출 방지를 위하여 적절한 보안성검토를 실시하여야 한다.

팀(부서)보안책임자

94) 팀 내 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 있음을 공지할 의무가 있다.

95) 퇴직(예정)자가 근무기간 동안 습득한 모든 영업비밀을 소속 팀(부서)에 인계 하도록 하고, 개인이 소지한 영업비밀은 회사에 반납 또는 재사용 불가한 상태로 파기하도록 요청하고 퇴직자 면담서류 등에 이에 대한 사항을 기록한다.

임직원

96) 임직원은 퇴직자가 동종업종 또는 경쟁사에 재취업하는 것을 인지하였을 경우 즉각 전사 보안담당부서에 통보해야 한다.

기술보안담당자 및 물리보안담당자

97) 퇴직 명령 일을 기준으로 24시간 이내에 퇴직자에 대한 출입 및 시스템상의 모든 접근 권한을 절차에 따라 모두 삭제 한다.

98) 정기적으로 퇴직자의 권한이 정상적으로 회수되고 있는지 현황을 확인하고 누락이 확인되면 그 원인을 확인하고 개선조치를 이행한다.

99) 업무인수/인계를 목적으로 팀(부서)보안담당자가 서면으로 요청하는 경우 최대 2주 기간 동안 권한 삭제를 유예할 수 있다. 권한 회수 유예로 문제가 발생하는 경우 팀(부서)보안담당자에도 책임이 있다.

100) 퇴직발령 게시 지연 등의 사유로 권한회수가 정상적으로 처리되지 않은 경우, 그 차이 기간 동안 출입/시스템 사용기록을 모두 확인하고, 팀(부서)보안담당자에 확인을 요청하고 그 결과를 포함하여 전사보안책임자(CSO)에 보고 한다.

보안 위반자 관리

보안위반 조치

101) 위반사항의 경중을 판단하여, 경미한 위반의 경우 전사보안관리자 명의의 주의조치를 해당 직원 및 소속 팀(부서)장에 통보하며, 중요한 위반이라고 판단되는 경우 전사보안책임자(CSO)보고 후 규정에 따라 조치한다.

102) 보안 위반에 대한 징계는 취업규칙과 인사규정 또는 보안규정에 정한 징계 종류 및 절차에 따른다.

103) 유사사고 재발방지를 위해 대책을 수립, 시행하고, 징계 결과는 임직원 전원에게 공지한다.

임직원

104) '정보보안 규정' 및 관련 지침/절차를 위반한 사실을 인지하는 경우 전사 보안주관부서에 즉시 위반 사실을 통보해야 한다.

105) 본인의 실수 또는 의도하지 않게 정보가 노출, 제공되었음을 확인하는 경우 전사 보안주관부서에 관련사실을 통보해야 한다.

위반자 경중 판단 기준

경미한 위반

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

107) 위반이력이 없는 임직원이 규정, 절차 등의 미 인지로 규칙/지침을 위반한 경우 중 중대한 위반의 사유가 되지 않는 경우

108) 본인의 위반사실을 통보해온 경우 중 중대한 위반에 사유가 되지 않는 경우

109) 위반회수에 따라 다음과 같이 조치를 상향 한다.

① 1 회 위반: 당사자 구두 경고

② 2 회 위반: 당사자 서면 경고(시말서) 및 팀(부서)장 구두경고

③ 3 회 위반: 당사자 및 팀(부서)장 서면 경고(시말서)

④ 4 회 이상: 고의적 정책 미 준수로 중대한 위반으로 상향

중대한 위반

인사징계위원회에 회부하여 경고 이상의 징계를 시행한다.

110) 고의로 보안 규정, 절차, 지침을 우회하는 행위를 한 경우

111) 보안사고와 직, 간접적으로 관련된 사안으로 인정되는 경우

112) 중대한 과실이거나, 동일한 위반을 반복적으로 지적 받는 경우

정보자산 분류

분류 주체 및 시기

113)-팀(부서)보안책임자는 회사의 자산분류 기준을 이해하고, 이를 바탕으로 정보자산 생성자가 최초분류를 시행하도록 공지, 점검한다.

114) 정보자산 생성자(임직원)는 정보자산 생성 시 분류기준에 따라 등급을 구분하여 회사 보안정책이 준수되도록 분류기준을 인지하고 관리한다.

115) 팀(부서)보안담당자는 팀 내 업무 변동사항 발생 시 2주 이내, 특별한 변동 사항이 없는 경우에도 연1회 정기적으로 정보자산 분류결과의 적절성에 대한 검토 및 조정을 시행한다.

정보자산의 구분

정보자산

116) 중요성 등급은 기밀성, 무결성, 가용성 측면에서 각 자산이 보안 위험에 노출되었을 경우 회사에 미치는 잠재적 손실 규모를 반영하여 측정한다.

117) 회사 내 정보자산에 대한 중요도는 주요 정보에 대해 기밀성, 무결성, 가용성 등의 보안요구사항을 고려하여 중요도 등급을 부여함으로써 이루어진다.

118) 정보자산 중에서 문서자산의 중요성 등급은 '7.2.2 보안문서'의 기준에 준한다.

보안문서

119) 보안문서는 대외비(Restricted), 비밀(Secret), 극비(Top Secret)로 등급을 구분한다.

120) 모든 보안문서는 당사 영업비밀로 구분되며 '8. 영업비밀(보안문서) 관리기준' 및 관련 규정을 준수해야 한다.

121) 대외비 문서는 모든 임직원이 사용할 수 있으나, 사외 유출시 회사에 손해를 끼치거나 해로운 결과를 초래할 우려가 있는 자료를 말한다.

122) 비밀 문서는 업무상 관련 있는 임직원만 제한적으로 사용이 허용되는 자료로, 사외 유출시 회사 중요정책의 효율적 집행에 지장 및 경제적 손실을 가져올 수 있는 자료를

말한다. 문서 생산자가 제한된 수신자를 지정하여 유통할 수 있으며, 임의로 복사 및 재배포할 수 없다.

123) 극비 문서는 비밀 등급의 문서보다 제한된 접근이 필요한 경우에 지정하며, 사외 유출시 회사 경영에 심각한 영향을 끼쳐 막대한 손해를 초래하는 자료를 말한다. 비밀 등급의 문서보다 제한된 접근이 필요한 경우 지정한다. 문서를 출력할 경우 모든 출력본에 문서정보를 기재하고 문서별 관리대장을 통해 해당 문서정보를 기록하고 폐기예정일에 따른 폐기 여부를 확인한다.

124) 임직원(계약관계에 있는 자 포함)에 의해 작성된 모든 문서는 재분류 전까지 대외비로 취급하며, 관련 규정을 준수 하여야 한다.

관리 및 소유권

125) 전사 보안주관부서는 팀(부서) 단위에서 작성할 수 있는 정보자산분류기준(템플릿)을 제공해야 한다.

126) 임직원은 보안문서 등급 분류 시 소속 부서 업무 단위로 등급을 부여하며, 이에 따른 관리 대장을 작성하여 운영해야 한다.

127) 전사 보안주관부서는 1 년에 1 회 이상 팀(부서)별로 파악된 정보자산의 리스트를 총괄 취합/관리하며, 과소, 과도 분류가 되지 않았는지 유효성 검증을 실시해야 한다.

128) 임직원, 외주업체, 제 3 자가 각각 혹은 공동으로 생산한 정보자산의 지적재산권은 별도 계약관계가 없는 경우 회사에 귀속된다.

영업비밀(보안문서) 관리기준

영업비밀의 분류

당사 영업비밀

129) 영업비밀은 최초 문서의 작성(기안)자가 분류한다.

130) 문서등급의 조정권한은 부서(팀)장 또는 상위 결재자에게 있으며, 문서의 유통범위에 대한 관리감독 책임을 가진다.

131) 문서의 내용이 보안문서와 일반문서가 혼합되어 있는 경우 상위등급의 내용으로 문서의 등급을 지정하여야 한다.

132) 영업비밀의 분류 시 분류기준 및 참고항목을 고려하여 등급을 결정해야 한다. 분류기준에 해당사항이 없는 경우라도 보안문서로 지정하여 관리할 수 있다.

타사 영업비밀

133) 제 3 자로부터 계약관계에 의해 타사의 영업비밀을 취득 시에는 제공자가 정당한 권한을 가진 자인가를 확인하여야 한다.

134) 타 회사에 근무경력이 있는 임직원은 이전 회사의 보안의무를 지고 있으므로 이전 회사의 영업비밀을 회사 내에서 공개, 사용하지 않아야 한다.

135) 업무적으로 제공받은 타사의 영업비밀은 제공자가 결정한 등급으로 분류한다.

136) 해당 등급이 없는 경우 차 상위등급으로 분류한다.

영업비밀의 이관

137) 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.

138) 팀(부서)별 보안책임자는 인계/ 인수 절차에 따라 영업비밀이 적절히 이관되었는지 확인하고 인계자 소유하고 있는 영업비밀이 모두 파기 되었는지 확인한다.

139) 업무상 이유로 기존 영업비밀의 일부를 전보된 부서에서 사용할 필요가 있는 경우 그 목적과 파일의 목록을 이전 팀(부서)보안책임자에 서면으로 보고 후 활용할 수 있다. 서면보고과정 없이 보유하는 경우 이유를 막론하고 고의적인 정보취득으로 보안위반자 처리규정에 따라 조치한다.

영업비밀의 배포 및 반출

140) 영업비밀을 본인의 업무와 직접적으로 관련이 없는 곳으로 반출할 사유가 발생하거나 국가기관 등 외부에서 요청한 자료의 범위에 영업비밀이 포함되는 경우 전사보안관리자의 사전 승인을 얻어 반출한다.

141) 본인의 업무 수행을 위해, 사외 반출하는 경우 반출처와 반출일시, 반출 내역을 회사가 정한 양식에 따라 작성하여, 주간 단위로 팀(부서)보안책임자에 보고하고, 결재를 받아 보관한다. 단, 기술자료(도면)를 배포/접수할 수 있는 시스템이 구축된 경우 별도의 기록을 작성하지 않고 시스템 로그로 대체한다.

142) 영업비밀의 반출 이력은 2년 이상 보관되어야 하며, 필요 시 쉽게 조회 가능한 상태로 관리되어야 한다. 사내 배포의 경우 영업비밀의 소유권자(작성자)의 판단에 따라 회사가 정하는 보호조치가 적용된 상태로 필요한 인원에 한정하여 배포한다.

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

보안문서의 보관 및 관리

144) 보안문서는 생성시 원본 문서에 해당 등급을 표기해야 하며, 생성과정에 있는 중간산출물 및 해당내용의 일부를 사용한 문서도 동일한 방법으로 관리되어야 한다. 기 생성된 문서 중 보안등급이 구분되지 않는 문서의 경우 소급하여 등급 분류를 시행한다.

145) 출력된 보안문서에는 그 등급이 매 페이지마다 쉽게 식별 가능하도록 표기 되어야 하며, 출력 시 표기하지 못한 문서의 경우 출력 후 고무인 등을 활용하여 표기한다. 그리고 개방된 장소에 보관해서는 안되며, 시건 장치가 있는 장소에 보관하고 팀(부서) 보안책임자가 지정하는 자가 관리한다. 또한 인식할 수 있는 관리자, 자산번호, 보관위치 등을 확인 할 수 있는 인덱스를 부착하여 관리해야 한다.

146) 전자상의 보안문서는 출력 시 문서열람 프로그램 또는 기타 시스템을 통해 워터마크 또는 회사 자산임을 증빙하는 문구를 포함하여 자동 출력되도록 해야 한다. 또한 파일 암호화, 보안이 적용된 저장공간 사용 등 회사에서 제공한 문서보안시스템을 적용하여 안전하게 보관해야 한다.

147) 보안문서는 업무목적 외에는 복사, 인용, 가공 등의 재생산을 해서는 안 된다. 보안문서의 재생산 시에는 당사 보안정책을 준수해야 하며, 전달받은 문서의 경우 전달자가 요구하는 보안사항을 이행해야 한다.

148) 영업비밀의 보호기간은 '부정경쟁방지 및 영업비밀보호에 관한 법률 2조 2항'에 정의된 영업비밀 충족요건이 유지되는 기간으로 한다.

149) 영업비밀 침해행위 및 기타 사유로 인해 영업비밀 충족여건을 상실하더라도 해당 문서의 중요도가 현저하게 감소하지 않는 경우 영업비밀에 준하여 관리되어야 한다.

보안문서의 파기

150) 출력된 보안문서는 보존기간이 만료되면 1 개월 이내에 복원할 수 없는 형태로 파기 한다. 단, 업무적 이유로 파기를 유예할 필요가 있는 경우 목적과 유예기간 등을 서면으로 보안 주관부서에 보고 후 보관한다.

151) 출력된 보안문서는 문서세단기를 사용하여 원형을 확인 할 수 없는 상태로 파기해야 한다. 임직원이 사용할 수 있는 문서세단기가 설치되지 않은 경우 전사보안책임자는 별도의 파기절차를 수립하여 운영해야 한다.

152) 문서의 파기는 해당문서의 생산자 및 사용자에 의해 임의로 실시해서는 안 되며, 반드시 소속 팀(부서)별 보안책임자의 책임하에 이루어져야 한다.

153) 전자상의 보안문서는 회사가 정하는 소프트웨어를 활용하여 복원 불가한 상태로 파기해야 하며, 사본도 같은 방법으로 파기 한다.

154) 전자문서 파기용 소프트웨어를 지정, 공지 하지 않은 경우 파기에 대한 책임은 전사보안책임자에 있다.

준거성

1.2. 전사보안관리자는 보안관련법령이 개정되거나, 고객사의 보안정책이 변경되는 경우 내부규정, 절차, 지침에 영향이 있는지 전사보안담당자를 통해 검토해야 하고 필요 시 개정해야 한다.

1.3. 검토 결과, 개정이 불필요하다고 판단되는 경우에는 검토 이력을 문서로 유지해야 한다.

1.4. 전사보안책임자는 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.

1.5. 기술보안담당자는 시스템의 취약점을 주기적으로 점검하여, 내부 규정 또는 외부 법령에 위반사항이 없도록 확인하고 개선이 필요한 경우 전사보안관리자, 전사보안책임자(CSO)에 보고하고 조치 한다.

보안점검

목적

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

시행 주체 및 주기

1) 전사보안책임자의 주관 하에 사전 계획에 따라 시행하며 점검을 시행할 인원은 전사보안관리자가 지명하고 전사보안책임자(CSO)가 승인한 임직원으로 한다.

2) 점검은 년 4 회 분기별로 시행한다.

3) 보안점검은 임직원의 일상적인 준수사항 위주로 시행한다.

4) 다음의 경우 상기 일정과 별도로 점검을 실시할 수 있다.

① 전사보안책임자(CSO)가 필요하다고 인정할 때

② 보안사고의 발생 우려가 있을 때 또는 보안사고 발생시

점검 대상

본 규정 1.2 적용범위에서 정한 범위를 대상으로 한다.

점검 시행

5) 임직원은 정당한 사유 없이 점검요청을 지연 하거나, 거부할 수 없다. 부득이한 경우 전사보안책임자(CSO)서면 보고 후, 승인된 경우에 한하여 일정을 조정할 수 있다.

6) 점검이 완료되면 전사보안관리자는 그 현황을 전사보안책임자(CSO)에 보고하고 [경미한 위반]으로 확인된 사항은 관련 팀(부서)보안책임자에게 개선을 요청 한다.

7) 팀(부서)보안책임자는 요구된 개선사항에 대한 조치방법/일정을 전사보안관리자에 회신하고, 계획에 따라 조치 후 완료여부를 전사보안관리자에 통보하는 것으로 개선조치를 종료한다. 조치는 통보 받은 시점부터 4 주 이내에 완료 해야 하며, 그 이상의 기간이 소요될 것으로 판단되는 경우 전사보안담당자를 통해 전사보안책임자(CSO)에 별도 보고 한다.

8) 전사보안관리자는 팀(부서)에 요청한 개선사항의 완료가 모두 확인되면, 전사보안책임자(CSO)에 점검에 대한 개선완료 보고한다. 단, 완료보고는 점검완료

시점부터 30 일을 초과 할 수 없으며, 4 주 이내 완료 통보하지 않은 팀(부서)는 '미조치'로 처리한다.

9) 전사보안관리자는 점검 결과 [중대한 위반]으로 판단되는 사항에 대해서는 전사보안책임자(CSO)보고 후 당사 규정에서 정한 절차에 따라 조치한다.

10) 모든 점검 결과 및 위반자 처리 결과는 3 년 이상 유지해야 한다.

11) 자체 점검을 이행하지 않거나, [중대한 위반]에 대한 조치를 소홀히 한 경우 전사보안책임자(CSO) 책임이 있으며, 고객사의 보안점검/감사 시 불이익의 사유가 될 수 있다.

제 3 장 물리적 보안

보호구역 설정

보호구역의 정의

1) 보호구역이라 함은 업무수행에 있어 비밀보호가 필요한 지역을 말하며, 그 중요도에 따라 '제한구역'과 '통제구역' 으로 구분하며, 보호구역의 세분화 관리를 위하여 '사업장구역'을 추가하여 구분할 수 있다.
2) 제한구역: 상주직원 이외에 출입이 금지되는 보안상 중요한 구역으로, 비 인가자의 출입을 방지하기 위하여 출입에 안내가 필요한 지역을 말한다.
3) 통제구역: 비 인가자의 출입이 금지되는 보안상 극히 중요한 구역으로, 비 인가자의 출입 시 사전에 반드시 관리책임자의 승인을 받아야 출입이 가능한 지역을 말한다.
4) 사업장구역: 비밀이나 중요시설, 자재 및 중요문서 등을 보호하기 위하여 일반출입자에 대한 감시가 요구되는 지역으로, 별도의 승인내역 없이 출입할 수 있는 구역이나, 회사의 보안관리범위에 있는 지역을 말한다.

보호구역의 지정

12) 사업장 보안책임자는 비밀보호의 중요도에 따라 보호구역을 지정하여야 한다.
13) 회사의 영업비밀 및 자산의 보호를 위하여 외부인의 출입을 제한하여야 하는 지역은 제한구역 이상으로 지정하며, 임직원 및 외부인은 절차에 따라 승인 후 출입한다.
14) 보호구역으로 설정된 지역은 비 인가자의 진입을 방지하기 위한 통제장치의 설치 및 보호활동을 하여야 하며, 출입기록을 유지하여야 한다.
15) 비밀보호를 위해 임직원의 출입을 통제하여야 할 필요가 있는 지역은 통제지역으로 지

정하며, 사진촬영 및 비인가 임직원의 출입을 제한한다.

16) 통제구역은 팀(부서)보안책임자의 의견을 수렴하여 물리보안담당자가 설정하고 전사보안책임자 및 전사보안책임자(CSO)에 보고 후 시행한다.

보호구역 표시

17) 보호구역의 출입 시 쉽게 확인이 가능한 출입문 중앙 또는 잘 보이는 곳에 부착한다.

18) 보호구역의 표지는 시설보호 및 출입통제지침 3.3.2항을 따른다.

출입관리

19) 임직원은 본인 근무지역 및 제한지역의 출입이 가능하며, 외부인은 회사 내 업무목적으로 필요한 경우에 방문을 요청하여야 하고, 방문신청은 외부인을 관리/통제할 수 있는 부서에서 신청 및 승인한다.

20) 외부인은 각 출입문 또는 안내데스크에서 신분확인 및 방문증을 수령하여 출입하여야 한다.

21) 업무적 계약이나 장기적으로 사업장내 출입하는 인원은 장기출입증 발급 후 출입하여야 한다.

출입증 운영

22) 임직원 출입증: 당사의 임직원에 한해 발급되는 출입증

- 사원증: 전 임직원 의무적 발급 및 출입의 목적으로 사용가능

23) 외부인출입증: 당사 임직원이 출입허가를 요청한 자에 발급하는 출입증

- 일일방문출입증: 외부인이 일일 사업장 방문 시 직원의 요청으로 발급하는 출입증
- 장기방문출입증: 업무적 계약 및 협력업체 등 장기적으로 출입하는 외부인에 발급되는 출입증으로 업체명, 성명, 사진, 출입기간이 포함된다.

24) 차량출입증: 사업장내 진입하기 위한 차량에 발급하는 출입증

- 임직원차량출입증: 출입승인은 받은 차량에 발급하며, 차량 전면유리에 부착
- 임시차량출입증: 사전 승인된 방문차량으로 일일차량출입증, 장기차량출입증으로 구분하여 발급하는 출입증

자산 반출·입 통제

반출·입 통제항목

1) 반출·입 통제 항목은 일반자산 및 정보자산으로 분류한다.
2) 일반자산 통제 항목
   - 생산 및 운영에 필요한 자재 및 부품, 완성품 또는 이에 준하는 자산
   - 기타 보안운영부서(팀)에서 선정한 일반자산
3) 정보자산 통제 항목
   - 컴퓨터 류(휴대형 포함), 서버 류, 저장매체 류 등의 정보처리 및 저장 장치 또는 이에 준하는 자산
   - 기타 보안운영부서(팀)에서 선정한 정보자산
4) 기타 통제하기 어려운 세부 항목에 대하여서는 보안운영부서(팀)에서 검토 및 선정하여 세부 지침에 명기할 수 있으나, 최소한으로 분류토록 한다.

반출·입 통제 관리

25) 당사 소유 및 비 소유 자산 등의 모든 통제 대상 자산에 대하여 사업장내 반출입시에는 반드시 해당 자산에 대하여 관리, 통제할 수 있는 부서(팀)의 승인 절차를 반드시 운영토록 한다.

26) 승인받은 외부인에 의한 자산 반출·입일지라도 업무 목적 이외의 행위를 할 경우 승인을 한 임직원에게도 책임이 있다.

27) 관리, 통제할 수 있는 부서(팀)의 승인이 있더라 하더라도 당사 보안 목적 달성을 저해하는 항목에 대하여서는 보안운영부서(팀)에서 반출·입을 통제할 수 있다.

CCTV운영 및 시설감시

기본원칙

1) 차량 및 인원이 출입하는 지역은 상시 감시하여야 한다.
2) 중요(보안)시설에 대하여는 CCTV 및 보안요원(인원)에 의한 감시를 하여야 하며, 사업장 특성에 따라 운영이 불가한 경우 무인경비시스템을 운영할 수 있다.
3) CCTV는 보안 및 화재, 도난 등에 대한 구체적이고 실질적인 위험 발생 우려가 있는 장소에 한하여 설치되어야 하며, 설치목적에 맞게 운영되어야 한다.
4) CCTV를 설치·운영할 때에는 주 출입구 등 쉽게 인지가 가능한 장소에 CCTV가 설치 운영 중임을 알아볼 수 있도록 안내판을 설치(부착) 하여야 한다.

관리책임

5) 물리보안담당자는 경비인력/CCTV의 관리 및 운영에 대한 책임을지며 업무를 위탁하는 경우 위탁계약서에 관계법령에 의거 개인정보보호에 관한 준수사항을 규정하여야 한다.

6) 전사보안관리자는 사업장 출입 등의 목적으로 수집된 개인정보 및 CCTV운영에 따라 수집된 영상정보에 대하여 물리보안담당자가 수집 목적 외 조작·유출 등 오남용 하지 않도록 관리·감독하여야 한다.

정보의 처리

7) 보관기간이 만료 된 개인정보(영상정보 포함)는 지체 없이 삭제하여야 하며, 복원이 불가능하도록 파기 하여야 한다.

8) 영상정보를 취급(모니터링)하는 장소 및 보관장소는 제한구역 이상의 보호구역으로 설정하여 관계자 외 접근을 통제하여야 한다.

9) 영상정보는 CCTV의 설치 목적 이외의 용도로 활용되거나, 접근권한을 부여 받은 자 이외의 타인에게 열람 제공되어서는 안 된다. 다만 법령에 의하거나 정보주체의 요청에 의하여 열람 및 자료를 제공하여야 할 경우에는 사전 전사보안책임자의 인가를 득해야 한다.

업무연속성 관리

업무연속성 관리절차 내 보안의 반영

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

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

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

1.5.5 업무연속성 계획은 정기적으로 테스트되고 그 유효성이 검증되어야 한다.

기타 세부 사항

1.5.6 본 규정에 언급되지 않은 사항 및 세부적인 내용은 '시설보호및출입통제지침', 'CCTV운영 및 시설감시지침' 및 '정보자산반출통제지침'에 따른다

제 4 장 기술보안

사용자보안지침

목적

1) 업무상 목적으로 회사에서 지급한 업무용 단말기의 정보기술보호를 위한 요구사항을 제공함에 그 목적이 있다.

관리항목

2) 업무용 단말기 도입, 운영 및 폐기에 대한 지침이 마련되어야 한다.
3) 업무용 단말기는 영문, 숫자 혼용으로 8자리 이상의 로그인, 화면보호기 비밀번호가 설정되어 있어야 한다.
4) 모든 PC에는 회사 업무용 목적으로 사용되는 회사에서 배포되는 프로그램만 설치가 가능하며, 불법 S/W 사용에 대한 책임은 본인에게 있다.
5) 모든 PC에는 악성코드 실행방지솔루션 등 보안시스템이 설치되어야 하며, 사용자는 최신 업데이트 및 최신보안패치 적용을 해야 하고, 그 현황이 유지되어야 한다.
6) PC내의 파일을 공유할 필요가 있을 경우, 비밀번호가 설정된 공유 폴더를 설정하여, 인가된 사용자만 접근할 수 있도록 해야 한다.
7) 공용PC에 대한 관리자를 지정해야 하며, 공용PC에는 보안문서를 저장할 수 없다.
8) 인터넷을 사용하는 경우 회사의 보안정책(접근차단시스템 등)을 준수해야 하며, 승인되지 않은 인터넷 망을 사용하여서는 안 된다.
9) 보안문서는 외부로 공중 네트워크(인터넷 등)를 거쳐 전송하는 것은 불허하며, 부득이한 경우는 사전 또는 사후에 관리자의 승인을 받아야 한다.
10) 사용자는 회사에서 지급한 H/W 및 S/W의 변경을 임의로 하여서는 안되며, 이동형 저장장치는 승인절차를 거친 후 사용해야 한다.
11) 모바일 기기로 업무를 수행하는 경우 관련 보안지침을 적용하여야 한다.

기타 세부 사항

12) '사용자보안지침'을 따른다.

네트워크보안

목적

13) 사내 네트워크 구성 및 외부 네트워크 연결 시 요구되는 정보기술보호의 수준을 향상시킴

으로써 안정적인 네트워크 인프라를 갖추는데 그 목적이 있다.

관리항목

14) 사내 네트워크는 외부에서 접근이 통제되는 별도의 네트워크를 구축해야 한다.
15) 외부에서 공중망을 통해 내부 네트워크로 접속하고자 할 경우, 암호화 및 인증 절차를 통하여 업무상의 목적으로만 사용해야 하며, 접근기록을 보관해야 한다.
16) 중요도가 높은 시스템 및 네트워크는 분리되어야 한다.
17) 허가되지 않은 전산장치의 회사 네트워크 사용을 금지한다.
18) 외부 방문객 또는 개인 PC의 네트워크 사용 시 정보기술보안관리자의 승인을 받은 후 사용해야 한다.
19) 신규 네트워크 설치 또는 구성 변경 시 테스트 등 검증 과정을 거친 후 승인절차에 의해 설치 및 변경해야 한다.
20) 인가되지 않은 무선 통신수단의 사용을 금지한다.
21) 인가된 무선 통신수단의 경우 적절한 통신 보호조치를 취하여야 한다.
22) 네트워크장비 설정 내용 백업 등 장애발생에 대비해야 한다.
23) 네트워크장비의 접근통제가 이루어져야 한다.
24) 네트워크의 도입, 운영, 폐기에 대한 지침이 마련되어야 한다.

기타 세부 사항

25) '네트워크보안지침'을 따른다.

시스템보안

목적

26) 시스템을 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운영 관리하는데 그 목적이 있다.

관리항목

27) 시스템의 도입, 운영, 폐기 프로세스에 대한 지침이 마련되어야 한다.
28) 시스템의 도입 및 변경은 적절한 절차에 따라 승인되어야 하며, 보안점검항목이 지정되어 있어야 한다.
29) 시스템 설치 시 기본적으로 생성되는 계정 및 사용하지 않는 계정은 삭제 및 변경되어야 하며, 반기 1회 전체 계정에 대한 검토를 실시하여야 한다.

30) 서버시스템에 접근한 기록은 3년 이상 보관되어야 한다.

31) 시스템 사용자 계정의 등록, 변경, 삭제는 공식적인 승인절차로 이루어져야 하며 이력관리가 되어야 한다.

32) 모든 사용자에게는 유일한 계정을 부여해야 하며, 계정공유현황을 분석해야 한다.

33) 비밀번호는 영문, 숫자 혼용 8자리 이상이며, 3개월 이내 변경되어야 한다.

34) 중요 업무 시스템은 개발과 운영시스템이 분리되어야 한다.

35) 어플리케이션의 개발 및 변경은 공식적인 승인 절차를 준수하여야 하며, 보안성 검토 및 기능 검증 테스트 후 운영에 반영되어야 한다.

36) 테스트데이터는 주민등록번호, 계좌번호 등과 같은 개인 정보 및 중요정보를 포함하여서는 안 된다.

37) 데이터베이스에 대한 접근통제가 이루어져야 하며, 접근로그를 3년 이상 보관해야 한다.

38) 시스템에 대한 주기적인 취약점 점검 및 조치가 이루어져야 한다.

39) 운영체제, 데이터베이스에 대한 백업 및 원격지 소산이 되어야 한다.

40) 시스템 장애에 대비한 복구계획이 마련되어야 하며 최소 년 1회 모의 훈련을 실시하여야 한다.

기타 세부 사항

41) '시스템보안지침'을 따른다.

보안시스템운영

목적

42) 보안시스템을 안정적, 효율적으로 운영 관리하기 위한 지침을 제공하는데 그 목적이 있다.

관리항목

43) 보안시스템의 도입, 운영, 폐기에 대한 지침이 마련되어야 한다.

44) 각 보안시스템에 대한 운용 매뉴얼을 마련하여야 한다.

45) 보안시스템은 인가된 사용자만이 접근해야 하며, 비밀번호는 영문, 숫자 혼합으로 8자리 이상으로 설정되어야 한다.

46) 보안시스템 관리자는 로그 기능이 항상 가동되도록 하고, 주기적으로 모니터링 및 분석해야 하며, 관련 로그는 3년 동안 보관해야 한다.

47) 보안시스템에 대한 취약점 분석을 주기적으로 시행하여 개선한다.

기타 세부 사항

48) '보안시스템운영지침'을 따른다.

IT보안사고관리

목적

49) IT 침해사고에 대한 대응 및 복구업무를 포함하고 있으며, IT인프라에 대한 피해를 최소화하고 재발 방지를 통하여 정보자산의 보안성과 안정성을 유지하는데 필요한 지침을 제공하는데 그 목적이 있다.

관리항목

50) IT보안사고 발생 시 기술보안담당자는 긴급히 대응하고, 그 처리 결과를 전사보안관리자 또는 전사보안책임자에게 보고해야 한다.

51) 사내의 모든 사용자는 침해사고 발견 시 즉시 기술보안담당자 또는 전사보안관리자에게 보고해야 한다.

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

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

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

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

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

57) 공개가 허용된 침해사고는 임직원에게 공지 또는 교육해야 한다.

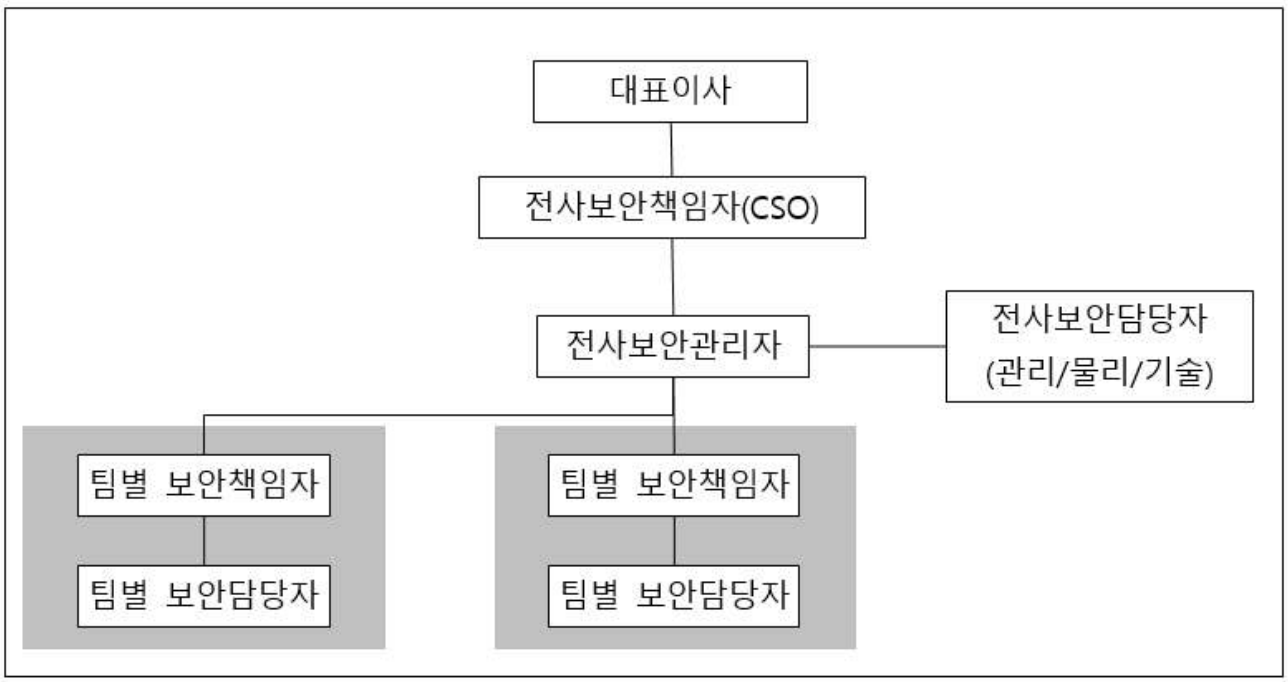
기타 IT보안사고

58) 'IT보안사고대응지침'을 따른다.

제 5 장 첨부

별첨

보안조직도



관련 지침 및 양식

관리영역

1.5.7 (HMG-ISSC-A-03) 글로벌표준보안규정양식

1.5.8 (HMG-ISSC-A-04) 개인정보보호지침

1.5.9 (HMG-ISSC-A-05) 모바일보안규정

물리영역

1.5.10 (HMG-ISSC-P-01) 시설보호 및 출입통제지침

1.5.11 (HMG-ISSC-P-02) CCTV운영 및 시설감시지침

1.5.12 (HMG-ISSC-P-03) 정보자산 반출입 통제지침

기술영역

1.5.13 (HMG-ISSC-T-01) 사용자보안지침

1.5.14 (HMG-ISSC-T-02) 네트워크보안지침

1.5.15 (HMG-ISSC-T-03) 시스템보안지침

1.5.16 (HMG-ISSC-T-04) 보안시스템운영지침

1.5.17 (HMG-ISSC-T-05) IT보안사고대응지