2024년도 용역사업 수행사 보안점검 체크리스트

용역수행사	
점검일자	
보안담당자	부서명 : 성 명 : (인)
점검결과	0.0

1. 관리적보안 (100점)

항목		점검내용	배점	해당여부 (O/△/X)	점수	근거자료명
1-1. 보안 관리 체계	1-1-1. 보안 관리 체계 운영	① 정보보안(관리적보안, 기술적보안) 관련 규정이 제정되어 있다.	5		0.0	
		② 시설보안 관련 규정이 제정되어 있다.	5		0.0	
		③ 문서보안 관련 규정이 제정되어 있다.	5		0.0	
		④ 인적보안 관련 규정이 제정되어 있다.	5		0.0	
		⑤ 보안규정에 보안활동과 관련된 조직 및 정보보호책임자가 명시되어 있다.	5		0.0	
		⑥ 보안규정 개정 시, 정보보호책임자의 승인 후 전 직원에게 공표한다.	5		0.0	
		⑦ 보안 관련 규정이 전직원에게 적용되고 있다. - 규정에 전 직원 적용 근거 없으면 감점 100%, 전 직원 적용 여부 현장실사 미 확인 시 감점 50%)	5		0.0	
	1-1-2. 보안 관리 체계 점검	⑤ 정보보안 규정이 회사 운영 현황과 일치한다. - 정보보안 규정과 회사 운영현황 현장실사 시 불일치 확인 시 감점 50%)	5		0.0	
		⑥ 시설보안 규정이 회사 운영 현황과 일치한다. - 시설보안 규정과 회사 운영현황 현장실사 시 불일치 확인 시 감점 50%)	5		0.0	
		⑦ 문서보안 규정이 회사 운영 현황과 일치한다. - 문서보안 규정과 회사 운영현황 현장실사 시 불일치 확인 시 감점 50%)	5		0.0	
		⑧ 인적보안 규정이 회사 운영 현황과 일치한다. - 인적보안 규정과 회사 운영현황 현장실사 시 불일치 확인 시 감점 50%)	5		0.0	
		⑨ 보안규정 개정 시, 정보보호책임자의 승인 후 전 직원에게 공표한다. - 보안규정 개정 시 정보보호책임자 미 승인 받거나 전 직원 미 공포 시 감점 50%)	5		0.0	
		⑩ 보안 관련 규정이 전직원에게 적용되고 있다.	5		0.0	
		⑪ 매년 단순 용어 변경 외에 최신 이슈를 반영하여 규정을 개정한다. - 악성코드 감염 등 이상 징후가 의심되는 경우 직원 행동지침 - 보안사고 발생 시 대응절차 - 악성코드 감염의심이 되는 경우 행동지침 등	5		0.0	
1-2. 보안 인식 개선 활동	1-2-1. 보안 교육	① 매년 정기적으로 전 직원 대상 보안교육을 실시하도록 규정에 명시되어 있고, 실제로 시행하고 있다. - 규정에 보안교육 실시 근거 없으면 감점 100%, 전 직원 보안교육 미 실시 확인 시 감점 50%)	4		0.0	
		② 한기 업무 수행 직원을 대상으로 사업 수행 전과 사업 수행 시 보안교육을 실시하고 있다. - 규정에 보안교육 실시 근거 없으면 감점 100%, 한기 업무 수행 직원 보안교육 미 실시 확인 시 감점 50%)	4		0.0	
		③ 신입사원, 퇴직예정자, 해외파견자, 사업참여자 등을 대상으로 특별 보안 교육을 실시한다. - 규정에 보안교육 실시 근거 없으면 감점 100%, 신입사원, 퇴직예정자, 해외파견자, 사업참여자 등 보안교육 미 실시 확인 시 감점 50%)	4		0.0	
	1-2-2. 보안 점검	① 연 1회 이상 자체 보안점검을 시행하도록 규정에 명시되어 있고, 실제로 시행하고 있다. - 규정에 보안점검 실시 근거 없으면 감점 100%, 자체 보안점검 미 실시 확인 시 감점 50%)	4		0.0	
		② 1-2-2-①에 의한 보안점검 이후, 지적 사항에 대한 개선 계획 및 재발방지대책을 수립하고 시행하고 있다. - 규정에 개선 계획 및 재발방지 대책 수립 근거 없으면 감점 100%, 개선 계획 및 재발방지 대책 미 수립 확인 시 감점 50%)	4		0.0	
		③ 1-2-2-②의 내용 (보안점검결과, 개선계획, 재발방지대책 등)을 보안점검 후 경영층에 보고하고, feedback을 받는다.	4		0.0	
	1-2-3. 보안 인식 수준	① 전직원이 보안사고 발생 시 대응 절차를 숙지하고 있다. (규정에 내용이 없으면 감점)	2		0.0	
		② 전직원이 악성코드 감염의심이 되는 경우 행동지침을 숙지하고 있다. (규정에 내용이 없으면 감점)	2		0.0	
		③ 전직원이 패스워드 규정 등 생활보안 준수사항을 숙지하고 있다.	2		0.0	

2. 기술적보안 (120점)

항목	항목	점검내용	배점	해당여부 (O/△/X)	점수	근거자료명
2-1.		① 업무망과 인터넷망을 물리적으로 분리 구성하여 업무를 수행하고 있다	10		0.0	
2-2. 전자메일 보안		① 메일 시스템 자료 보안 메일 관련 서버를 직접 운영하거나 호스팅 서비스를 받고 호스팅 업체의 보안대책을 증빙할 수 있는 경우 (상세 보안대책 내용은 가이드북 참조) - 자체 메일이 있는대 상용메일(다음, 네이버 등)을 이용하여 용역자료 수발신 시 감점 50% - 전자메일을 이용하여 용역자료 수발신 시 첨부파일 암호화미 실시한 경우 감점 50%)	10		0.0	
2-3. 단말기 보안	2-3-1. 백신 프로그램	① 백신 프로그램을 정식 구매하여 모든 PC에 설치하여 운영 중이다.	3		0.0	
		②-1. 백신 업데이트 패치 파일을 전사에 강제로 적용할 수 있는 솔루션을 운영하거나, 수동으로 패치 업데이트를 진행하고 관리대장을 기록하고 있다.	5		0.0	
		②-2. 백신 업데이트를 강제로 적용할 수 있는 솔루션은 없으나, 수동으로 패치 업데이트를 진행하고 관리대장을 기록하고 있다.				
		③ 백신 정책을 중앙에서 통제할 수 있는 솔루션을 운영하고 있다.	5		0.0	
	2-3-2. 계정 및 공유 폴더 관리	① PC에 불필요한 계정(Guest, Owner, Test, Admin, ASPNET 등)은 없거나 비활성화 되어 있다. - 망분리 운영 내부망 PC인 경우 감점 50%, 인터넷망 PC인경우 감점 100%)	6		0.0	
		② PC에 기본공유(C$, D$, Admin$ 등)를 사용하지 않는다. - 망분리 운영 내부망 PC인 경우 감점 50%, 인터넷망 PC인경우 감점 100%)	6		0.0	
		③ 공유 폴더를 사용하지 않는다. [불가피 할 경우 반드시 암호 설정 후 사용 (암호 저장 금지)]	5		0.0	
	2-3-3. 패스워드 및 화면보호기	① 윈도우 패스워드 규정을 준수하여 패스워드를 설정한다. (규정에 내용이 없으면 감점100%)	5		0.0	
		② 부팅 패스워드(CMOS)를 규정을 준수하여 패스워드를 설정한다. (규정에 내용이 없으면 감점100%)	5		0.0	
		③ 규정을 준수하여 10분 이상 자리 이석 시 PC단말기 화면보호기를 설정하고 있으며 재시작 시 로그인 하도록 되어있다. (규정에 내용이 없으면 감점100%)	5		0.0	
	2-3-4. PC 관리	① 보안에 취약한 OS · 브라우저 등을 사용하지 않는다.	5		0.0	
		② 인터넷이 연결된 PC에 한기 문서 및 도면 등의 용역사업 관련 자료를 보관하지 않는다. - 망분리 운영 미 적용 시 암호를 설정하여 용역 수행 관련 자료를 보호한다 - 인터넷이 연결된 PC에서 암호 미설정 용역자료 확인 시 감점100%	10		0.0	
		③ P2P, 메신저, 웹하드, 유해사이트, C&C서버 등에 접속을 제한하는 솔루션을 운영하거나 직접 유해싸이트를 제한하고 있다.	10		0.0	
2-4. 저장매체 관리		① PC에 저장매체 연결 시, 백신프로그램을 통해 자동 검사가 진행된다.	5		0.0	
		② 용역 수행을 위해 저장매체 사용 전 발주처로 부터 사전 승인을 받고 사용하고 있다. - 현장 실사에서 사전 승인여부 확인 미 승인받고 사용 시 감점 100%)	10		0.0	
		② 저장매체 연결 필요 시 보안USB를 사용하고 있다. - 현장 실사에서 저장매체 사용 이력 확인 후 보안USB 미 사용 시 감점 100%)	10		0.0	
		③-1 매체제어시스템을 운영하여 저장매체 연결을 통제하고 있다.	5		0.0	
		③-2 매체제어시스템을 운영하지 않지만 저장매체 시 관리대장에 사용내역(사용자, 사용일시, 사용목적, 사용매체 인식번호 등)을 승인받고 관리하여 저장매체 연결을 통제하고 있다.				

3. 물리적보안 (60점)

항목	점검내용	배점	해당여부 (O/△/X)	점수	근거자료명
3-1. 시설보안	① 감사 대상 장소의 출입문 등에 시건장치가 설치되어 있다.	3		0.0	
	② 사무실 내로 외부인이 출입하는 경우, 별도의 출입 절차가 있다.(최소한 보안대책: 외부인 출입관리대장 및 관련 규정) - 규정에 내용이 없으면 감점100%	3		0.0	
	③ 보호구역이 보호구역 운영조건을 준수하고 있다. (보호구역 운영조건 중 50% 이상 충족 시 인정) - 규정에 내용이 없으면 감점100%	5		0.0	
	④ 전산장비(PC, 노트북, 서버 등) 반출 시, 보안사고 예방을 위한 보안 절차가 있다. - 규정에 내용이 없으면 감점100%	6		0.0	
	⑤ 고장 등의 사유로 전산장비를 파기하여야 하는 경우, 데이터 복구가 불가능하도록 파기한다. - 규정에 내용이 없으면 감점100%	5		0.0	
3-2. 문서보안	① 문서 관련 규정에 한기 관련 문서·도면·계산서 등이 보호 대상으로 지정되어 있고, 보호 대상 문서에는 보안 등급을 부여하여 관리하고 있다. - 규정에 내용이 없으면 감점100%	5		0.0	
	② 보안등급이 부여된 문서를 보관하는 캐비닛, 서랍장 등에 시건이 되어 있다. - 규정에 내용이 없으면 감점100%	5		0.0	
	③ 캐비닛 및 서랍장 등에 관리자(정/부)가 지정되어 있다. - 규정에 내용이 없으면 감점100%	3		0.0	
	④ 사무실에 파쇄기가 설치되어 정상적으로 운영되고 있고 폐지(사용용도가 종료된 문서 자료 및 휴지 등)는 파쇄하여 처리한다. - 규정에 내용이 없거나 현장 실사 시 폐지가 휴지통 등에 존재하면 감점100%	5		0.0	
3-3. 인적보안	① 내부직원 및 외부직원의 입·퇴사 시 보안각서를 징구하고 있다. - 현장 실사 시 누락 인원 확인되면 감점100%	10		0.0	
	① 재직 중인 내부직원 및 외부직원의 보안각서를 매년 징구하고 있다. - 현장 실사 시 누락 인원 확인되면 감점100%	10		0.0	

4. 필수 교육이수 및 이행점검 (20점) - 추후 자료 취합 및 확인 후 점수 반영함(한전기술 작성)

항목	점검내용	배점	점검 점수	점수
4-1. 필수 교육 이수	① 발주처에서 실시하는 보안교육을 이수하였다. Ex) 교육 참석 1회당 5점	10		0.0
5-1. 이행점검	② 한기 보안점검 결과에 대한 조치 이행 계획 제출 및 이행 여부가 확인되었다. - 조치이행계획 없는 경우(0점) - 조치이행계획 제출(5점) - 조치계획에 대한 이행여부확인 결과(5점)	10		0.0

5. 기타 사항

- 체크리스트 점검항목 외 추가 보안활동 및 취약점 개선 참여 시 가점 부여(한전기술 작성)

- 보안점검 결과 이행조치 요구 미 이행 시 감점

항목	점검내용	배점	점검 점수	점수	
5-1. 취약점 개선 참여	① WIPIMS 및 3D CAD 등 한기 정보시스템 사용 시 보안 취약점을 발견하여 발주처 담당자에게 조치 의뢰한 실적이 있다.(개선조치 의뢰 건당 가점 5점)			0.0	
5-2. 추가보안활동	① 체크리스트 점검항목 외 용역사 자체적으로 수행한 추가 보안활동 실적이 있다고 판단되는 경우 (추가 보안활동 실적 건당 가점 5점 부여)			0.0	
5-3. 이행조치 미 이행	① 발주처에서 요구하는 보안취약점 조치 및 보안점검 결과 보안취약점 조치 미이행 - 조치 미 이행 건당 5점 감점			0.0	

6. WIPIMS 및 3D CAD 사용 업체 필수 이행 사항(미충족 시 감점 / 해당 시스템 미사용 시 미해당)

항목	항목	점검내용	배점	해당여부 (O/X)	근거자료명	근거자료명
6-1. VPN 장비	6-1. VPN 장비	① WIPIMS 및 3D CAD 연결을 위한 VPN장비가 존재한다.	-5		0.0	
		② WIPIMS 및 3D CAD 연결을 위한 VPN장비가 통제 가능 구역에만 존재한다.	-5		0.0	
		③ 관리자(사내직원) 이외의 직원(외부인 포함)이 VPN 설정 값 변경을 하지 않는다.	-5		0.0	
6-2. 단말기 관리	6-2. 단말기 관리	① WIPIMS 및 3D CAD 단말기에서 인터넷을 사용하지 않는다.	-10		0.0	
		② WIPIMS 및 3D CAD 사용 및 한기업무 수행을 위한 프로그램 외 불필요한 프로그램을 사용하지 않는다.	-5		0.0	
		③ WIPIMS 및 3D CAD PC의 로컬디스크(일반적으로 C/D Drive)에 한기문서가 존재하지 않는다.	-5		0.0	
		④ WIPIMS 사용자를 관리대장에 기록/관리하고 있다. (필수항목: 계정명, 이름, 사용기간, 사용목적, 해지날짜, 승인)	-5		0.0	
		⑤ 3D CAD 사용자를 관리대장에 기록/관리하고 있다. (3D CAD 미사용 업체는 해당 없음) (필수항목: 계정명, 이름, 사용기간, 사용목적, 해지날짜, 승인)	-5		0.0	
		⑥ WIPIMS 및 3D CAD용 단말기를 지정된 사용자 외의 직원이 사용하지 않는다.	-10		0.0	
6-3. 봉인 관리	6-3. 봉인 관리	① USB포트, 랜포트, SATA포트 등 저장매체 연결이 가능한 포트 및 단말기 개봉에 대한 자체적인 통제를 효과적으로 시행하고 있다.	-10		0.0	
		② 승인되지 않은 저장매체(USB, 외장HDD, SATA DISK, 핸드폰 등)의 연결 기록이 없다.	-5		0.0	

※ 각 체크항목에 대한 상세 내용 설명은 "보안활동가이드북V03" 참조

※ 실사감사대상장소 : 실제 한국전력기술 업무 수행 공간

※ 체크리스트의 내용은 대·내외 여건을 반영하여 변경될 수 있으며, 변경사항은 변경 시 통보 예정

※ 공인된 ※ 공인된 정보보호경영체계(ISMS 또는 ISO27001 인증서) 보유 시 별도 제출