|  |
| --- |
|  |
| 제21회 정보보호 대상 심사기준 및 평가항목 |
|  |

**□ 서류심사 기준 및 평가항목**

|  |  |  |
| --- | --- | --- |
| **평가 항목 및 내용** | | **배 점** |
| 비즈니스 경쟁력  및 사회 기여도 | 기업의 연혁, 조직구성 및 인지도 | 20점 |
| 기업의 보유 특허 및 국제 인증, 신용도 평가 |
| 기업의 사회적인 책임여부 |
| 정보보호 부문 일자리 창출 |
| 인터넷 이용환경 개선 여부 |
| 정보보호 관리  및  기술 우수성 | 정보보호정책을 위한 기반마련 | 40점 |
| 정보보호 관리정책의 구성 및 준수여부 |
| 정보보호 기술대응조치 |
| 정보보호 물리보안여부 |
| IT예산 대비 정보보호예산 비율 |
| 정보보호  수준향상 | 정보보호 인식제고 활동(정보보호 유관기관 가입 유무) | 40점 |
| 정보보호 관련 수상실적 및 우수사례 |
| 위험 대비 및 정보보호 관련 대외활동(해커톤 등) |
| CEO 정보보호 활동 참여 및 관심 |
| 조직 및 인력, 정책, 기술, 모의훈련 / 모의해킹 |
| 악성코드 유포/경유지 악용여부 및 관리ㆍ대응 현황 |
| 가점 | - 정부정책 이행 여부  ㆍISMS, PIMS, ISMS-P 및 ISO27001 인증여부  ㆍ정보보호 준비도 평가 이행여부  ㆍ정보보호 공시제도 이행여부  - 버그바운티 제도 운영 여부  - 기타 독창적인 보안활동 등  ※ 각 항목 1개 이행 시 1점씩 가점 (총 5점) |  |
| **합 계** | | **100점** |

**□ 현장심사 기준 및 평가항목**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | **주요 점검 내용** | **배점** | **점수** | **비고** |
| 1. 정보보호 최고책임자(CISO) 지정과 책임 권한여부 | - 정보보호 최고책임자 지정 여부  - 정보보호 최고책임자 자격, 활동 평가  - 독립적인 정보보호 전담조직 설치 여부활동평가  - 정보보호 최고책임자의 권한 확보 여부 | 5점 |  |  |
| 2. 정보보호 의사소통 및  정보제공 | - 정보보호 홍보활동 및 외부자문활동  - 정보보호담당자와 실무자간 의사소통  - 정기적인 정보보호 회의  - 최고경영진과의 정보보호사항 논의 | 5점 |  |  |
| 3. 정보보호정책 유무  /구현/시행 등 | - 정보보호 정책 문서 존재 여부  - 정보보호 운영방침의 CEO서명 및 공표, 게시여부  - 조직운영방침에 맞는 정책 개정 여부  - 정보보호정책 위반에 따른 상벌규정 포함 | 4점 |  |  |
| 4. 정보보호추진계획  수립 및 이행여부 | - 정보보호 목표수립과 추진계획 문서화  - 연간 정보보호 활동, 책임자의 참여도 | 4점 |  |  |
| 5. 정보보호 전담조직  구성 및 운영 | - 정보보호담당자 지정의 문서화  - 정보보호 전담조직의 경력/자격 및 전문성 강화  - 정보보호 전담조직 적정 인력 구성 | 4점 |  |  |
| 6. 정보보호 예산 집행 | - 정보보호 예산 수립과 CEO의 승인  - 정보보호 활동 부분 할당량  - 주기적 실적 검토, 정보보호활동 이행실적 등 | 4점 |  |  |
| 7. 정보보호 활동 점검, 감사 수행 | - 최소 연 1회 이행점검 수행  - 점검 항목의 적절성과 이행점검 결과 실천  - 이행점검 수행조직의 전문성, 독립성 | 4점 |  |  |
| 8. 정보보호 교육 수행 | - 연간 정보보호 교육 계획에 따른 수행 여부  - 전체임직원 및 외부위탁사 대상 교육  - 업무특성에 따른 교육 내용 구분  - 교육참여 독려 제도 | 5점 |  |  |
| 9. 정보자산 관리 | - 정보자산 목록 및 구성현황 관리  - 보안등급 식별기준 정책 마련  - 자산 변경사항 기록 관리  - 정보자산의 주기적인 관리 | 4점 |  |  |
| 10. 인적보안 활동 | - 입사/퇴사시 정보보호 서약서 징구  - 인사 이동시 해당 권한 회수  - 주요직무자 지정, 관리 및 정보보호 준수사항 상기 활동 | 4점 |  |  |
| 11. 외부 위탁 및 용역 시 보안 관리 | - 외부계약 위탁 시 정보보호서약서 징구  - 계약서 등에 보안요구사항 명기 여부  - 외부자 업무 종료 시 보안활동 이행 점검  - 법률 요구사항을 고려한 보안관리 정책 수립  - 월 별 보안사항 점검 수행 | 5점 |  |  |
| 12. 취약점 점검 및 개선 | - 취약점 점검계획 수립 여부  - 조직이 관리하는 전체 정보시스템 점검  - 정보보호 취약점 점검인력의 전문성  - 연 2회 이상의 점검 수행  - 점검 결과 개선조치 및 CISO 결과 보고 여부 | 5점 |  |  |
| 13. 정보보호 사고탐지 및 대응 | - 침해사고 탐지 시스템 운영 및 이벤트 기록 유지  - 조직, 역할, 대응절차, 비상연락체계 등의 문서화  - 침해사고 발생을 대비한 지속적 모니터링 수행  - 정보보호 사고 유형에 따른 대응방안 마련  - 매년 침해사고 대응 체계 점검 모의 훈련 실시 | 5점 |  |  |
| 14. 시스템 개발 보안 | - 시스템 개발 시 개발환경 보안  - 안전한 코딩 규칙 적용 등 개발 보안 조치 여부  - 개발자의 전문성 및 취약점 점검/조치 | 4점 |  |  |
| 15. 네트워크 보안 | - 침입차단, 네트워크 분리, 인터넷차단 등 보안설정 | 4점 |  |  |
| 16. 정보시스템 및 응용 프로그램 인증 | - 정보시스템/어플리케이션 접속단말 지정  - 정보시스템/어플리케이션 원격접근 통제, 사용자인증 강화  - 보안정책 또는 지침수립/점검 | 5점 |  |  |
| 17. 자료 유출 방지 | - 중요정보 유출을 대비한 전송 및 저장시 암호화  - 중요정보 유출 방지 탐지, 보안시스템, 대책 마련  - 정보유출에 대한 적극적인 대응 | 4점 |  |  |
| 18. 시스템 및 서비스 운영보안 | - 악성코드에 대한 대책 적용  - 정보시스템 보안패치, 서버 백신 설치  - 운영로그의 기록 및 보관  - 원격작업에 대한 대책마련, 통제 수행 | 5점 |  |  |
| 19. 백업 및 IT 재해복구 | - 백업대상 시스템과 데이터 정기적 백업 수행  - 중요 백업데이터 물리적 보관  - 실시간 백업 체계 완비  - 연 1회 이상의 재해복구 훈련 | 4점 |  |  |
| 20. PC 및 모바일기기 보안 | - PC관리 점검사항 배포 및 점검  - PC보안조치 중앙 시스템 구축/운영  - 모바일 기기 보안지침 마련 | 4점 |  |  |
| 21. 정보통신시설 환경 보안 | - 보호구역 지정과 보호대책 문서화  - 화재, 전력공급, 온도, 습도 설비 설치/관리 | 4점 |  |  |
| 22. 정보통신시설 출입 관리 | - 출입통제 장치 유무, 기록, 모니터링  - 노트북, 서버 등 반출입 통제 | 4점 |  |  |
| 23. 사무실 보안 | - 비인가자의 출입통제  - 중요문서 보관  - 정기적인 사무실 보안점검 수행 | 4점 |  |  |
| **합 계** | | **100점** |  |  |

|  |  |
| --- | --- |
| **참고** | **정보보호 대상 신청서 양식** |

**제21회 정보보호 大賞 신청서**

**□ 기업 개요**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 기 관 명 |  | | | | | | | | | | | |
| 소재지(주소) |  | | | | | | | | | | | |
| 대표자 성명 |  | 홈페이지 | |  | | | 사업자  등록번호 | | |  | | |
| 총 종사자 수 | 명 | 정보화(IT)  전담인원 | |  | | | 정보보호  전담인원 | | |  | | |
| 담당자 성명 |  | | 근무부서 | |  | | | | 직 위 | | *※ 임원 또는 부장 급 이상* | |
| 전화번호 |  | | 이메일 | |  | | | | 핸드폰 | |  | |
| 정보보호 현황 | ISMS/PIMS/ISMS-P/ ISO27001 인증여부 | | 전담부서 지정 | | | CISO지정 | | IT예산 대비  정보보호예산 비율 | | | | 정보보호 정책 이행 여부 |
|  | |  | | |  | |  | | | | *※ISMS, PIMS, ISMS-P 준비도 평가, 공시* |
| 수상내역 | •  •  • | | | | | | | | | | | |

※ 수상내역은 3개 이내로 기재(정보보호 대상 수상경력이 있을 경우, 필히 기재)

**□ 정보보호 활동(공적)**

|  |  |
| --- | --- |
| **지원동기** | *※ 정보보호 대상에 지원한 동기(수상 목적, 수상 후 활용방안 등)를 기재하여 주시기*  *바랍니다.* |
| **비즈니스 경쟁력 및 사회기여도** | *※ 기업에 대한 자유로운 소개(기업 신용도평가 등)와 사회적 책임(CSR) 등 사회기여에 관련된 내용을 기재하여 주시기 바랍니다.*  <평가항목> - 제출 시, 삭제 부탁드립니다.  o 기업의 연혁, 조직구성 및 인지도  o 기업의 보유 특허 및 국제 인증, 신용도 평가  o 기업의 사회적인 책임여부  o 정보보호 부문 일자리 창출  o 인터넷 이용환경 개선 여부 |
| **정보보호 관리 및 기술 우수성** | *※ 정보보호 관리 : 위험관리 방법론 자체보유 여부, 정보보호 인력 현황, IT예산대비 정보보호 예산 비율 및 투자 실적 등을 포함하여 기재하여 주시기 바랍니다.*  *※ 정보보호 기술 : 정보보호 개발기술, 기능 및 성능 기술개발전략 등을 포함하여 기재하여 주시기 바랍니다.*  <평가항목> - 제출 시, 삭제 부탁드립니다.  o 정보보호정책을 위한 기반마련  o 정보보호 관리정책의 구성 및 준수여부  o 정보보호 기술대응조치  o 정보보호 물리보안여부  o IT예산 대비 정보보호예산 비율(최근 3년간 예산 기준) |
| **정보보호 활동사항** | *※ 정보보호 인식제고 실적 : 대내외 정보보호 활동 실적 및 정보보호 인식 향상 교육 등을 포함하여 기재하여 주시기 바랍니다.*  *(예시. 정보보호 캠페인, 보안제품 무료 배포, 보도자료 배포, 대내외 정보보호 교육 등)*  *※ 정보보호 모범사례 : 정보보호 관련 수상실적, 정부정책 이행 여부 등을 포함하여 기재하여 주시기 바랍니다. (추가 증빙자료 첨부 가능)*  <평가항목> - 제출 시, 삭제 부탁드립니다.  o 정보보호 인식제고 활동  o 정보보호 관련 수상실적 및 우수사례 |
| **침해사고 대응력** | *※ 침해사고로 인한 피해 경험과 이에 대한 대응 사례를 자유롭게 기재하여 주시기 바랍니다.*  *피해경험 및 대응 사례가 없으면 침해 사전 대응을 위한 노력(위의 정보보호 관리 및 기술 우수성의 내용을 추가 보완)을 기재하여 주시기 바랍니다.*  <평가항목> - 제출 시, 삭제 부탁드립니다.  o 조직 및 인력, 정책, 기술, 모의훈련 / 모의해킹  o 악성코드 유포/경유지 악용여부 및 관리ㆍ대응 현황  o 정부정책 이행여부  - ISMS, PIMS, ISMS-P 및 ISO27001 인증, 정보보호 준비도 평가, 정보보호 공시제도  o 버그바운티 제도 운영 여부  o 기타 독창적인 보안활동 |