

# 정보보안 관리실태 평가 소개

## 국가사이버안전센터

### 요 약

국가 정보보안 정책 이행실태 확인을 통해 각급기관이 체계적으로 정보보안 업무를 수행토록 지원하고 국가·공공기관 종사자의 보안의식을 함양함으로써 각급기관 정보보안 수준 제고 및 국가 사이버안전 확보한다.

공공기관을 감독하는 주무 행정기관에 공공기관 보안평가 결과 통보, 부처 산하기관 대상 정보보안 관리 강화한다. 보안평가 우수기관 대상 보안업무 유공포상 실시하며 보안평가 결과는 국가 정보보안 정책 수립 시 기초자료로 활용한다.

### I. 목 적

국가 정보보안 정책 이행실태 확인을 통해 각급기관이 체계적으로 정보보안 업무를 수행토록 지원하고 국가·공공기관 종사자의 보안의식을 함양함으로써 각급기관 정보보안 수준 제고 및 국가 사이버안전 확보한다.

### II. 법적 근거

- ◎ 「국가정보원법」 제3조 제2항(직무)
- ◎ 「전자정부법」 제56조(정보통신망 등의 보안대책 수립·시행) 제3항
- ◎ 「전자정부법」 시행령 제69조(전자문서의 보관·유통 관련 보안조치)
- ◎ 「전자정부법」 시행령 제70조(보안조치 이행여부의 확인)
- ◎ 「공공기록물 관리에 관한 법률」 시행령 제5조(전자기록물의 보안관리)
- ◎ 「국가사이버안전관리규정」 제9조(사이버안전대책 수립·시행 등) 제4항
- ◎ 「국가정보보안기본지침」 제12조(정보보안 관리실태 평가)

### III. 추진 경과

- ◎ 2004년 정보보안 관리수준 평가제도 도입
- ◎ 2006년 50개 국가기관 대상 시범평가 실시

- ◎ 2007년 교육청 포함 99개 국가·공공기관 대상 평가 실시
- ◎ 2008년 정부출연 연구기관으로 대상 확대, 117개 국가·공공기관 대상 평가
- ◎ 2009~2010년 공기업으로 대상 확대, 145개 국가·공공기관 대상 평가
- ◎ 2011년 147개 기관은 사이버안전센터에서 직접 평가하는 한편, 감독부처를 통해 부처 산하기관 간접평가를 병행하여 총 800여개 국가·공공기관 대상 평가
- ◎ 2012년 준정부기관으로 대상 확대, 199개 국가·공공기관 대상 평가
- ◎ 2013년 120개 국가·공공기관 대상 평가

### IV. 평가 방법

- ◎ 정보보안 관리실태 평가는 기관이 자체평가를 실시하고 그 결과의 객관성·공정성을 담보하기 위해 국가사이버안전센터가 현장실사를 실시한다.
- ◎ 최종 평가결과에 대한 공신력 제고를 위해 민·관 전문가로 구성된 평가위원회에서 평가결과의 적정성을 심의한다.
- ◎ 국가사이버안전센터는 국가정보보안 정책, 평가분석 결과, 사이버위협 실태 등을 반영하여 매년 평가 기준·항목 등을 수정·보완하여 평가에 적용한다.
- ◎ 정보보안 관리실태 평가는 다음의 5단계로 이루어진다.

평가 단계	주 체
① 기관별 자체평가	각급기관
② 현장실사	국가사이버안전센터
③ 결과분석 및 점수산출	국가사이버안전센터
④ 평가결과 심의·의결	평가위원회
⑤ 최종 평가결과 통보	국가사이버안전센터

(그림 1) 정보보안 관리실태 평가 단계

#### 4.1. 기관별 자체평가

- 평가 대상기관은 국가사이버안전센터가 구축한 온라인 평가시스템의 계정을 부여받아 정해진 기간 동안 각 평가항목별 자체평가를 실시한다.
- 각급기관은 자체평가의 적절성을 입증할 수 있는 평가항목별 증빙자료를 준비하여 국가사이버안전센터의 현장실사시 제출하여야 한다.
- 각급기관은 평가내용 입력시 관련 사항을 증빙할 수 있는 문서·사진 등 관련 자료를 온라인 평가 시스템에 첨부할 수 있다.
- 자체평가 기간 중 각급기관 참여하에 사이버안전센터 주관 해킹메일 대응훈련을 실시하고 훈련결과를 평가에 반영한다.

#### 4.2. 현장실사

- 국가사이버안전센터는 각급기관의 자체평가에 대한 객관성·공정성 확보를 위해 해당 기관을 방문하여 자체평가 결과를 검증한다
- 현장실사 평가반 구성시 전문성과 객관성을 담보하기 위해 學·研 전문가를 참여시킬 수 있다.
- 자체평가와 현장실사 결과가 상이하여 평가점수가 변동될 경우 해 기관 정보보안담당관의 확인을 받아 객관성을 확보한다.
- 평가 대상기관은 자체평가를 증빙할 수 있는 자료 및 면담을 위한 직원을 배치하여 신속한 현장실사가 이루어질 수 있도록 한다.

- 실사반은 직원의 보안의식 확인을 위해 일반직원을 임의 선정하여 정보보안 기본수칙·사이버침해사고 대응절차 숙지 여부 등을 확인하고 PC 보안관리 실태를 점검한다.
- 국가사이버안전센터는 현장실사시 대상기관이 제출한 서류·문건 등에 대해 종료 후 반납함을 원칙으로 한다. 다만, 국가사이버안전센터가 필요하다고 판단된 경우에는 사본 1부를 제출 받을 수 있다.

#### 4.3. 결과분석 및 점수산출

- 평가지표를 기준으로 산출된 현장실사 점수와 정성 평가점수를 일정 비율(매년 변동 가능)로 합산하여 최종 평가점수를 산출한다.
- 평가점수는 점수에 따라 우수(90이상), 양호(80이상), 보통(70이상), 미흡(60이상), 불량(60미만)의 5단계로 구분한다.
- 정성평가 점수는 該 기관의 연간 해킹사고 발생현황, 사이버위기대응 통합훈련 결과, 정보보안 우수사례, 평가준비 사항(정성평가) 등을 종합하여 반영한다.
- 국가사이버안전센터는 기관별 현장실사 등 평가결과를 종합 분석, 우수·미흡 분야를 도출한다.
- 평가결과를 다각도로 심층 분석하여 연도별, 평가지표별, 보안요소별, 보안활동 주체별 보안수준을 도출하고 기관의 보안활동 중점 방향을 발굴한다.

#### 4.4. 평가결과 통보

- 국가사이버안전센터는 기관별 정보보안 관리실태 평가결과를 평가 대상기관과 정부업무평가 주관기관인 기재부, 안행부 등에 통보한다.
- 평가 대상기관은 국가사이버안전센터가 통보한 평가결과를 자체 정보보안 대책 등에 반영, 미흡점을 개선·보완하여 정보보안 수준을 제고하여야 한다.
- 국가사이버안전센터는 평가결과 공통적으로 드러난 보안 취약요소 보안을 위해 국가 정보보안 정책에 개선대책을 반영하는 한편, 차년도 정보보안 관리실태 평가시 이를 집중 점검한다.

(표 1) 평가지표 분류표

분 야	평 가 지 표	항 목
1. 정보보안 정책(20)	1.1 정보보안 규정 및 계획	3개
	1.2 정보보안 조직 및 인원	5개
	1.3 정보보안 기본활동	6개
	1.4 기관장 관심도	3개
	1.5 주요정보통신기반시설 보호	3개
2. 정보자산 보안관리 (23)	2.1 정보자산 승인 및 관리	4개
	2.2 용역사업 관리	9개
	2.3 국가용 보안시스템	3개
	2.4 보호구역 관리	4개
	2.5 휴대용 저장매체 관리	3개
3. 인적 보안(14)	3.1 내부인원 보안	2개
	3.2 외부인원 보안	5개
	3.3 정보보안 교육	7개
4. 사이버위기 관리(16)	4.1 사이버위기 관리체계 구축	2개
	4.2 예방활동	5개
	4.3 사이버위기 대응훈련	5개
	4.4 사이버침해사고 대응·복구	4개
5. 전자정보 보안(26)	5.1 비밀의 전자적 관리	4개
	5.2 전자우편 보안	3개
	5.3 웹서비스 보안	6개
	5.4 전자정보 유출 방지	7개
	5.5 사용자 인증	4개
	5.6 클라우드 컴퓨팅 보안	2개
6. 정보시스템 보안(30)	6.1 정보보호시스템 보안	6개
	6.2 무선랜 보안	3개
	6.3 네트워크 보안	4개
	6.4 정보시스템 운용관리	6개
	6.5 PC 보안	7개
	6.6 로그 및 백업	4개
합 계	29개 지표	129개

V. 평가결과 활용

- ◎ 국가·공공기관 정부업무평가에 '정보보안 관리실태 평가 결과' 반영
- ◎ 대통령 비서실 및 국가안보실에 보안평가 결과 통보, 대통령 보고
- ◎ 공공기관을 감독하는 주무 행정기관에 공공기관 보안평가 결과 통보, 부처 산하기관 대상 정보보안 관리 강화
- ◎ 보안평가 우수기관 대상 보안업무 유공포상 실시
- ◎ 보안평가 결과는 국가 정보보안 정책 수립시 기초 자료로 활용