## 1. 침해사고시 통지의 내용 및 방법

### - [참조 자료] 02. 침해사고관리지침_Ver 1.0 ( 6 페이지 - 제 7조 침해사고 보고 3항)

③ 침해사고 발생 시 법률이나 규정 등에 따라 관계기관 및 이용자(정보주체) 에게 신고하여야 한다.

1. 통지방법 : 전화, 휴대전화, 전자우편, 서비스접속화면등 방법으로 제시함

2. 발생내용

3. 발생원인

4. 서비스 제공자의 피해확산 방지 조치 현황

5. 서비스 이용자의 피해예방 또는 확산방지 방법

6. 담당부서 및 연락처

## 2. 침해사고 대응절차 및 사후관리 대책

### - [참조 자료] 02. 침해사고관리지침_Ver 1.0 ( 6 페이지 - 제 8조 침해사고 대응)

**제8조(침해사고 대응)**

① 정보보호 침해사고 접수 후 정보시스템별 담당자는 침해사고 유형별로 다음 각 호의 절차에 따라 대응한다.

1. 침해사고가 확대되지 않도록 침해당한 서버의 네트워크 분리, 공격 포트의 차단 등 필요한 응급조치를 먼저 취한다.

2. 침해사고의 확산을 막기 위해 해당 정보시스템의 중단이 통계청 전체 업무에 영향을 미치는 경우 업무시간 종료 후에 서비스를 중단하며, 해당 정보시스템의 중단이 일부 업무에 영향을 미치는 경우에는 해당 업무부서와 협의 후 즉시 해당 정보시스템을 중단시킨다.

3. 응급조치 후 정보보호 침해사고의 원인 분석 및 증거확보를 위하여 해당 침해사고 관련 로그 및 제반 증거자료를 수집 및 확보해야 한다.

4. 국가정보원 등에서 권고하는 유형별 대응 조치를 취하고, 추후 재발방지를 위한 교육 등 대응책을 마련해야 한다.

② 정보보호 침해사고 유형에 따라 다음과 같이 구분한다.

1. 악성코드 공격

2. 서비스거부 공격

3. 비인가접근 공격

4. 복합구성 공격

- [참조 자료] 02. 침해사고관리지침_Ver 1.0 ( 8,9 페이지 - 제 13조 사후관리)

**제 13 조(사후관리)**

① 정보보호 관리자는 유사한 사고의 재발 방지를 위하여 관련 정책 및 지침의 개정, 정보보호시스템 도입, 유관기관 협조체계 구축 등 효과적인 재발방지 대책을 수립하여야 하고, 필요 시 보안사고 대응절차에 대한 내용을 변경하여야



한다.

② 정보보호 관리자는 수립된 재발방지 대책을 보고하여 동일 또는 유사 사고의 재발에 대비하여야 하며 보안사고의 대응 및 복구가 완료되었음을 확인하여야 한다.

③ 정보보호 담당자는 1, 2 등급의 보안사고 관련된 기록을 대외비 이상 등급으로 분류하고, 이를 보존·관리하여야 한다.

④ 법적 또는 규정상 보안사고 관련하여 대외기관의 요청이 있는 경우 대외협력 관련부서는 정보보호 관리자와 협의 후 대응하여야 한다.

⑤ 정보보호 관리자는 보안사고에 대한 정보와 발견된 취약점들을 관련 부서 및 임직원들에게 공유 및 전파하여야 한다.