**<1 Shop 정보보호 관리 현황 인터뷰 자료>**

**◎ 인터뷰 개요**

|  |  |  |  |
| --- | --- | --- | --- |
| 부서명 | 정보보호 파트 | 인터뷰 일시 | 10월 1일 |
| 담당자명 | 최보안 | 참석자 | 담당자 포함 3명 |

**◎ 인터뷰 주요 내용**

|  |
| --- |
| **Q :** 정보보호 정책 관리 방법은?  A : 최고경영자(나최고)의 승인을 받음. 정보보호 활동을 정의한 정책 1종과 세부내용이 들어있는 지침 4종 보유하고 있으며, 정책과 지침간의 연계성을 위해 연 1회 지침 검토 중  **Q :** 정보보호 조직 체계는?  A : 정보보호 정책을 통해 대표이사와 임원급의 책임을 명시하고, 정보보호 관련 업무는 임원급의 승인을 요하기 때문에 무중단 서비스 제공 및 회원들의 프라이버시 보호 고려. 보안 부서는 없지만 정보보호 파트, 정보보호 책임자, 정보보호 관리자 등이 지정됨  Q. 입사자와 퇴사자에 대한 정보보호 지침의 적용?  A. 신규 입사자의 경우 업무 투입전 보안교육을 필수로 받아야 하며 업무에 대한 적격성 검토 및 정보보호 서약서 작성이 요청됨. 별도의 계정 신청서를 작성하고 담당부서장의 승인 이후 계정이 발급됨. 물론 퇴사 시에도 정보보호 서약서를 별도로 작성하고 있고, 계정을 비롯하여 자산 반납 등이 이뤄짐  Q. 사내 중요정보(알고리즘 개발)에 대한 임직원의 접근 권한이 설정 기준은?  A. 임직원 그룹웨어 사용 권한은 부서별로 차등 부여하고 있음. 이 기준에 따라 네트워크, 서버에 대한 접근이 차등화되며, 최소한의 접근권한만 부여하게 되어 있음. 인프라 부서 이외의 부서 직원은 인사부서 또는 인프라 부서를 통해 그룹웨어 계정 발급  Q : 주요 업무를 처리하는 담당자에 별도의 관리 기준이 존재하는지?  A : 1 Shop은 망분리 대상이지만 아직 망분리가 적용되지 않음 다만, 임직원의 인식제고를 통하여 외부로의 자료전송은 금지하도록 교육 실시. 또한 임직원이 보유하는 PC의 악성코드 감염을 위하여 유해사이트 차단 시스템을 통해 인터넷 접속을 제한 중. 또한 DRM 솔루션을 이용하여 자료를 모두 암호화 처리하고 외부의 전송이 필요한 경우, 부서 장의 승인 획득 요구  Q : 침해사고 발생 및 대응 경험이 있는지  A : 보안관제업체를 통하여 침해사고 모니터링을 수행 중이며, 침해사고 유형별 분류, 유형별 보고 대응, 복구 절차 등 침해사고대응 지침을 수립하고 신속한 대응 및 처리를 위해 침해사고 대응조직 및 비상연락 체계 구성 중. 그리고 악성메일 모의훈련을 통해 악성파일, 랜섬웨어 등 메일을 통한 내부 침투에 대비하는 모의훈련도 실시 중.  다만, 매년 악성코드 감염 등의 사고는 지속적이고 반복적으로 발생하는 중임. 최근 3년 동안 내부 랜섬웨어 감염 사례가 지속적으로 발생하여. 일부 회원 정보가 복구되지 않은 사례 존재.  Q : 로그 관리 및 취약점 점검 현황은?  A : 각 서비스별로 모든 사용자의 접근 및 자원 이용에 대한 로그는 삭제없이 저장하고 있음. 주요 로그에 대해서는 별도 백업 서버에서 실시간 저장하고 있음. 인프라 장비(OS/ DBMS/네트워크/보안장비)에 대한 취약점 점검 및 모의해킹을 취약점 점검은 연 1회 점검하고 1개월 이내 취약점 조치 적용.  Q. 자연재해, 해킹 등과 같은 IT재해 재해 발생 시 대책 존재 여부?  A : 아직까지는 화재나, 홍수 등은 발생한 적은 없지만 비상 상황에 대비해 복구조직, 비상연락체계 등이 포함되어 있는 IT재해복구 체계가 구축되어있고, 재해복구 지침도 수립되어있습니다. |