|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 주식회사 유라클 | | | | | 사규규정표지 | | | | 등록번호 : | | | 영업비밀-19-02 | | |
| 개정차수 : | | | 1차 | | |
| **보안관리규정** | | | | | | | | | | | | | | |
| 제정 정보 | | | | | | | | | | | | | | |
| 제정일자 | | | 2019년 1 월 20 일 | | |  | 구분 | 작성 | | 검토 | | | 승인 | |
| 시행일자 | | | 2019년 2 월 1 일 | | | 결 | 직책 | 차장 | | 전무 | | | 대표이사 | |
| 작성부서 | | |  | | | 재 | 성명 | 서강남 | | 권태일 | | | 조준희 | |
| 협조부서 | | |  | | |  | 일자 | 19.01.31 | | 19.02.01 | | | 19.02.01 | |
| 개정 이력 | | | | | | | | | | | | | | |
| 차수 | 개정일 | 시행일 | | 주요 개정내용 | | | | | 작성 | | 검토 | | | 승인 |
| 1 | 19.01.20 | 19.01.20 | | 최초 작성 | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |
|  |  |  | |  | | | | |  | |  | | |  |

**보안관리규정**

|  |  |
| --- | --- |
| 2019년 1 월 20 일 | 제정 |

**제1장 총칙**

**제1조 (목적)**

이 규정은 주식회사 유라클(이하 “회사”라 함)의 정보자산 및 보안사항, 기타 회사정보를 다양한 위험으로부터 보호하며, 불법적인 정보 유출을 사전에 예방하여 회사의 기업가치 및 정보자산의 손실을 최소화하기 위해 필요한 사항을 규정함을 목적으로 한다.

**제2조 (정의)**

이 규정에서 사용되는 용어의 정의는 다음과 같다.

1. “정보”라 함은 회사의 경영 또는 활동에 필요한 일체의 지식을 말한다.
2. “정보시스템”이라 함은 회사가 보유하고 있는 컴퓨터(PC, 노트북 등), 서버, 휴대용 저장매체, 통신기기, 전산시스템, 네트워크장치, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
3. “정보자산”이라 함은 업무수행과 관련한 “정보시스템”과 업무결과 산출되는 “정보” 등을 포괄한 개념을 말한다.
4. “영업비밀”이라 함은 그 내용이 누설 또는 유출될 경우 회사에 유해한 결과를 초래할 우려가 있어 통제 및 관리가 필요한 모든 사항으로서 <영업비밀 관리규정>에 따라 비밀로 분류 및 취급, 관리되는 기술상 또는 경영상 정보를 말한다.
5. “보안”이라 함은 발생 가능한 모든 정보유출 및 다양한 위험으로부터 회사의 가치 있는 정보를 보호하며, 회사의 기업비밀이 관계자 외 또는 타 경쟁업체에 공개 혹은 누설되지 않도록 취하는 유형, 무형의 모든 예방조치를 말한다.
6. “시스템관리부서”라 함은 “정보시스템”의 도입 및 유지, 관리를 총괄하는 부서이다.
7. “각급기관”라 함은 회사 규정에 의하여 설치된 각종 하부 및 소속기관(교육기관, 연구기관, 연수기관 등을 포함한다)을 말한다.

**제3조 (적용범위)**

이 규정은 다음 각 호를 그 적용범위로 한다.

1. 회사에 신규채용·재직·퇴직하는 모든 임직원
2. 회사의 각급기관
3. 용역, 하청, 고객 등 회사와 계약관계에 있는 자
4. 회사의 외부 협력업체와 파트너
5. 기타 회사를 출입하는 모든 사람

**제4조 (임직원의 역할과 책임)**

1. 정보보안의 주체는 임직원 개개인이며, 회사의 기업비밀을 효과적으로 보호하고 불법 유출을 예방하기 위한 역할과 책임도 임직원 개개인에게 있다.
2. 정보보안에 대한 관리는 각 주무부서에서 하는 것을 원칙으로 하며, 각 부서장(이하 “보안책임자”)이 보안관리의 책임을 진다.
3. 보안책임자는 정보보안 업무수행을 위하여 이 규정의 범위 내에서 부서 실정에 적합한 별도의 대책을 마련하여 시행할 수 있고, 부서 내 보안담당자를 지정하여 보안업무의 일부를 위임할 수 있다.
4. 전사적으로 사용되는 서버 및 전산시스템, 네트워크장치, 응용프로그램 등 공용 정보시스템에 대한 보안 책임은 시스템관리부서에 있다.

**제5조 (보안업무의 분류)**

1. 회사의 모든 정보에 대해 ‘일반업무’와 ‘보안업무’로 구분하고, ‘보안업무’는 다시 ‘시스템보안업무’와 ‘일반보안업무’로 구분된다.
2. ‘시스템보안업무’는 컴퓨터, 정보통신망 등 주로 컴퓨터를 통하여 진행되는 정보시스템에 관한 보안업무를 말하며, ‘일반보안업무’는 그 이외의 모든 부문의 정보보안업무를 말한다.

**제6조 (정보 공개의 제한)**

1. 회사의 정보 중 영업비밀은 대외적으로 비공개를 원칙으로 하며, 임직원은 그 보유 및 취급, 관리에 있어 <영업비밀 관리규정>에 따라 외부에 공개되지 않도록 주의하여야 한다.
2. 예외적으로 영업비밀을 공개할 경우에는 <영업비밀 관리규정>에 따라 엄격한 절차를 준수하여야 한다.

**제7조 (정보자산의 소유권)**

임직원이 회사 근무 재직 중 업무와 관련하여 직·간접적으로 생산하거나 획득한 모든 정보자산에 대한 권리는 회사에 있다.

**제8조 (처벌 사항)**

1. 임직원이 비밀준수의무를 위반하여 회사의 허락을 득하지 않고 회사의 직무와 관련된 기사 자료 제공, 기고, 인터뷰, 외부강연, 도서출판, 방송출연 등의 행위를 하였을 경우에는 인사규정에 따라 징계하며, <부정경쟁방지 및 영업비밀보호에 관한 법률> 등 관련 법령에 따라 민·형사상의 책임을 진다.
2. 징계의 종류 및 징계사항, 징계위원회 구성, 징계심의 등은 인사규정에 따른다.

**제2장 인원 보안**

**제9조 (임직원의 비밀준수의무)**

1. 전 임직원은 회사에서 정한 비밀유지서약서를 작성, 제출하여야 하며, 선량한 관리자의 주의의무로서 회사의 비밀정보를 취급하고, 비밀유지 의무를 준수하여야 한다.
2. 회사에서 근무 재직하는 동안 취득하거나 지득한 정보 및 영업비밀은 회사의 자산으로서, 이를 업무수행 이외의 목적으로 사용하거나 제3자에게 공개 또는 제공하지 않으며, 부정한 목적으로 사용하지 않는다.
3. 회사의 전 임직원은 회사의 정보자산을 보호하며, 이 규정에 따른 제반사항을 준수하고 성실히 이행하여야 할 의무가 있다.

**제10조 (퇴직자 관리)**

1. 보안책임자는 퇴직자 관리를 위해 다음과 같은 보안성 조치를 취하여야 한다.
2. 퇴직 전까지 퇴직자에 대한 보안교육을 실시한다.
3. 공용시스템 접근통제(ID삭제 등) 등의 조치를 해당 부서에 요청하여야 한다.
4. 정보유출 우려 시에는 퇴직 전이라도 인터넷 및 네트워크 차단 등을 해당 부서에 요청하여야 한다.
5. 컴퓨터, 정보저장매체 및 기타 자료에 대한 보안 조치를 강구하여 회사의 정보자산이 반출되지 않도록 해야 한다.
6. 인사부서에서는 퇴직발령이 확정되면 시스템관리부서에 그 현황을 통보하여야 한다.
7. 시스템관리부서에서는 퇴직자의 컴퓨터(PC, 노트북 등)에 대한 반납 등의 보안 조치를 취하여야 하고, 퇴직자의 회사 네트워크 접속 및 관련 계정을 즉시 차단 및 삭제되도록 조치하여야 한다.

**제11조 (교육훈련)**

1. 교육관련 부서에서는 이 규정에서 정의하는 목적에 대해 주기적으로 회사의 임직원 및 용역업체 직원들에게 정보 보안 인식을 제고시킴으로서 자발적인 보안관리 및 예방활동을 이행할 수 있도록 한다.
2. 교육내용은 보안규정, 보안 인식 제고, 관련 법령 및 법적책임, 사고사례, 임직원 보안관리 사항, 정보보안 준수사항 등을 포함한다.

**제3장 문서 보안**

**제12조 (문서의 정의)**

1. “문서”라 함은 회사 각 부서간 또는 대외적으로 업무상 작성, 시행되는 일체의 서류(도면, 사진, 디스크, 자기테이프, 필름, 슬라이드 및 정보저장매체 등의 특수매체기록을 포함한다)와 회사에 접수된 모든 대외문서를 말한다.
2. “문서”는 전자문서 및 종이문서, 비밀문서, 일발문서로 구분되며, 그 정의는 다음과 같다.
3. “전자문서”라 함은 업무수행을 위하여 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 저장되거나 송·수신된 문서형식의 자료로서, 각종 정보저장매체 및 정보시스템에 수록, 저장되거나 또는 네트워크 장비, 통신 선로를 통하여 송·수신되는 형태의 것을 포함한다.
4. “종이문서”라 함은 “전자문서”가 프린터 등의 출력장치에 의해 종이에 출력된 서류 및 수기로 작성된 서류 등 모든 종이 문서를 말한다.
5. “비밀문서”라 함은 “영업비밀”이 포함된 “문서”를 말한다.
6. “일반문서”라 함은 “영업비밀”이 포함되지 않은 “문서”를 말한다.

**제13조 (비밀문서의 관리)**

1. 비밀문서는 반드시 ‘대외비’를 표시하며, <영업비밀 관리규정>에 따라 분류 및 관리한다.
2. 비밀문서는 보관함을 비치하여 보관하며, 반드시 시건장치를 하여야 한다.
3. 비밀문서 보관함 외부에는 ‘비밀문서’임을 나타내는 표시는 하지 아니하며, 일반문서 보관함과 같이 관리번호와 보관책임자를 명시한다.

**제14조 (일반문서의 관리)**

일반문서도 보안의 대상이 되므로 무단으로 공개하여서는 아니 되며, 외부에 공개할 자료 중 중요한 사항은 반드시 해당 부서장의 승인을 받아 공개한다.

**제15조 (문서 관리책임자)**

각 부서장(보안책임자)은 부서업무와 관련된 문서의 관리책임자로서 다음 각 호의 임무를 수행하여야 하며, 부책임자(보안담당자)를 정하여 관리책임자 부재 시 그 임무를 대리하게 한다.

1. 문서를 최선의 상태로 보관한다.
2. 문서의 도난, 유출, 분실 및 기타 손괴 등의 방지를 위하여 감독한다.
3. 비밀문서 보관함을 관리하고, 시건장치의 열쇠를 보관한다.
4. 비밀문서에 대해서는 취급 및 사용을 승인하고, 적정한 사유가 발행하면 파기한다.
5. 비밀문서에 대해서는 <영업비밀 관리규정> 및 <영업비밀 등급별 관리지침>에 따라 관리한다.

**제4장 정보시스템 보안**

**제16조 (컴퓨터의 사용 및 관리)**

1. 임직원은 회사가 각 개인에게 제공한 컴퓨터를 회사의 업무 행위를 위해서만 사용하여야 한다.
2. 컴퓨터의 계정 및 패스워드 관리는 다음과 같다.
3. 컴퓨터 접속 계정의 공유를 금하며, 공유로 인한 책임은 계정의 원소유자에게 있다.
4. 컴퓨터 사용자는 부팅 패스워드를 설정하여야 하며, 일정시간 자리를 비울 경우 자동적으로 화면보호기가 작동되도록 해야 한다.
5. 패스워드는 타인에게 공개 또는 방치해서는 안되며, 패스워드의 관리 소홀로 인한 책임은 사용자에게 있다.
6. 패스워드가 유출 또는 도용되었음을 인지한 경우, 즉시 이를 변경하여야 한다.
7. 컴퓨터 사용자는 업무용으로 지급된 컴퓨터 및 주변장치의 도난, 분실, 파손 및 오용으로 인한 정보유출 등에 대하여 관리 책임을 진다.
8. 컴퓨터 사용자는 시스템관리부서의 승인없이 컴퓨터를 임의로 분해할 수 없으며, 인가 받지 않은 장시 또는 장비를 부착, 설치할 수 없다.
9. 회사 내 모든 컴퓨터 사용자는 불법 소프트웨어를 사용해서는 안 되며, 불법 소프트웨어를 사용함으로 인한 모든 책임자는 사용자 본인에게 있으며, 회사는 책임이 없다.
10. 회사 내 모든 컴퓨터 사용자는 바이러스 침입 및 해킹을 방지하기 위한 소프트웨어와 각종 보안 솔루션을 설치하고, 정기적으로 백업 및 업데이트 관리를 하여야 한다.

**제17조 (통신망의 사용 및 관리)**

1. 임직원들은 회사 내에서 공통으로 사용하는 통신망만을 사용하여야 한다.
2. 이메일의 사용은 회사의 표준메일시스템 사용을 원칙으로 하며, 임직원들은 회사에서 부여한 이메일 계정 사용해야 하고, 회사에서 사용을 금지한 이메일을 사용해서는 안 된다.
3. 이메일 사용에 있어 메일서버의 안정된 운영을 위하여 주기적으로 확인된 메일은 삭제하여야 한다.
4. 인터넷의 사용은 회사 업무와 관련된 것들에 한정되어야 하며, 보안책임자 또는 영업비밀관리책임자는 회사의 영업비밀 보호 및 업무 효율성 확보를 위해 인터넷상의 특정 사이트 접속을 통제할 수 있다.
5. 회사 내에서 P2P통신프로그램의 사용은 금지되며, 관련 사이트는 모두 차단한다.
6. 임직원들은 외부로 문서를 발송할 경우에는 각 부서장의 사전 승인을 받아야 한다. 단, 전결권한이 있는 임직원은 그렇지 아니하다.

**제18조 (서버의 사용 및 관리)**

1. 영업비밀을 보관 또는 처리하는 서버는 강화된 사용자 인증 기능을 사용한다.
2. 서버 내 정보에 대한 접근권한은 업무적으로 필요한 범위 내에서만 허용한다.
3. 시스템 데이터에 대한 접근은 인가된 최소한의 사용자에 대해서만 허가한다.
4. 모든 중요 서버에 대해서는 보안도구를 적용하여 접근통제를 수행하여야 하며, 프로그램 소스에 대해서는 엄격한 접근통제가 이루어져야 한다.
5. 모든 서버는 백업 및 복구에 관한 절차가 수립되어야 한다.

**제19조 (정보시스템 관리)**

1. 보안책임자는 회사의 정보시스템을 연1회 이상 정기적으로 점검하고, 그 결과를 전체 임직원에게 공개한다.
2. 임직원들은 회사의 정보시스템에 대한 보안 문제를 발견한 즉시 시스템관리부서 또는 보안책임자에게 그 사실을 신고하여야 한다.
3. 시스템관리부서에서는 회사의 정보자산 보호 및 영업비밀에 관한 정보 유출 방지를 위한 관리의 목적으로 다음 사항에 관한 각종 통신기록 등을 모니터링 할 수 있다. 단, 사적인 개인정보는 모니터링 대상에서 제외된다.
4. 회사의 표준메일시스템을 통한 사외 메일 발송
5. 인터넷 접속(웹메일, 웹하드 등)을 통한 자료 전송
6. 통신프로그램(메신저, P2P, FTP 등)을 이용한 자료 전송
7. 가상사설망(VPN) 등
8. 다음에 해당할 경우, 시스템관리부서에서는 해당 직원의 인터넷 등네트워크의 사용을 일정기간 차단 또는 제한할 수 있다.
9. 회사의 중요 정보자산을 네트워크를 통해 외부에 유출하거나 허가 없이 공개한 경우
10. 허가되지 않은 매체 또는 방법을 사용하여 외부와 통신한 경우
11. 정보보호를 위해 시스템관리부서에서 불가피하다고 판단될 경우(예컨대, 불법S/W사용, 바이러스 설치, 해킹프로그램 사용이 확인된 경우 등)

**제20조 (음성·영상 통신 정보보안)**

회사의 모든 정보는 음성통신 또는 영상통신을 통하여 외부로 유출되어서는 안된다.

**제21조 (물품 등의 반입, 반출)**

1. 회사에 물품, 기기 등을 반입·반출하는 임직원은 보안책임자의 사전승인을 얻어야 한다.
2. 컴퓨터, 노트북 등 정보처리장치(휴대용을 포함) 및 USB메모리, 외장 HDD 등 전자기록매체 등을 사용하고자 하는 임직원은 사전에 보안책임자 또는 시스템관리부서의 승인을 얻어야 하며, 회사의 업무를 위해서만 사용하여야 한다.
3. 반입·반출이 금지 또는 제한된 컴퓨터 또는 전자기록매체를 반입·반출하는 경우, 이를 사용하는 사용자는 반입·반출일자, 기기사양, 사용용도, 사용자 정보 등을 작성하여 보안책임자에게 제출하고, 보안책임자는 이를 직접 확인한 이후 사용자가 제출한 서류를 시스템관리부서에 제출하여야 한다.
4. 시스템관리부서의 관리담당자는 전항의 서류를 별도로 보관하고, 회사 내의 컴퓨터 및 전자기록매체 등의 존재 및 사용현황을 수시로 확인하여야 한다.

**제22조 (정보시스템 보안점검)**

1. 시스템관리부서는 주기적으로 보안 진단의 날을 정하여 다음 사항을 중심으로 보안 관리 현황에 대한 점검을 실시하여야 한다.
2. 컴퓨터 진단프로그램 점검결과 및 보안패치 등 취약점 제거 확인
3. USB메모리 등 전자기억매체 관리현황 점검
4. 시스템관리부서의 관리담당자는 각 부서의 보안관리실태를 점검하기 위하여 야간 불시점검을 실시할 수 있다.
5. 보안책임자는 전항의 점검결과 보안관리 상태가 불량한 임직원에 대하여는 엄중 문책 또는 경고조치를 하여야 한다.

**제23조 (침해사고 대응)**

시스템관리부서에서는 정보시스템에 대한 바이러스 침투, 해킹 등 주요 정보 침해사고 발생에 대비한 대응절차 및 대응책을 수립하여야 한다.

**제5장 시설 보안**

**제24조 (출입증 패용 및 출입절차)**

1. 방문객은 출입방문증을 패용하여야 한다.
2. 회사의 사무실 및 공장에 출입하는 모든 출입자들은 출입절차 및 통제에 적극 따라야 한다.

**제25조 (보호구역)**

회사는 다음과 같이 보호구역을 설정하여 운영한다.

1. 제한구역 : 회사의 정보보호를 위하여 외부인의 출입이 제한되며, 관계자의 안내를 받아 출입하여야 하는 구역(예컨대, 통신실, 기계실, 공장 등)
2. 통제구역 : 회사 내 보안상 극히 중요한 구역으로 관계자 외 모든 출입자의 통제가 요구되는 구역(예컨대, 연구실, 전산실, 서버실, 영업비밀 보관실 등)

**제26조 (통제구역 관리)**

1. 통제구역은 인가된 최소한의 직원만이 출입할 수 있도록 엄격히 제한하며 관계자 외 출입 시에는 엄격한 통제가 요구된다.
2. 통제구역은 ‘통제구역’이라는 표시를 필히 해당 구역에 부착한다.
3. 통제구역으로 설정된 지역 또는 공간은 이중 시건장치 등 출입통제 장치를 강화하여 설치, 운영하여야 한다.
4. 연구실, 전산실, 서버 및 전산장비 등 중요 정보자산을 보유한 건물이나 장소는 주변으로부터 물리적, 환경적으로 안전하게 보호하여야 한다.

**제27조 (보안시스템 운영)**

1. 외곽시설, 주차장 등 주요 지역에 적절한 감시장비를 도입·운영하여야 한다.
2. 회사 내 모든 보호구역에는 출입을 관리할 수 있는 출입통제시스템을 도입·운영하여야 하며, 통제구역에는 기본적인 출입통제시스템 외에 이중적 보안장치를 설치하여야 한다.
3. 회사 내 정보자산의 도난 및 불법외부 유출을 방지하기 위한 보안장비와 솔루션을 적절히 설치·운영하여야 한다.
4. 신규 보안시스템 도입 시에는 회사 네트워크 및 기존 보안시스템과의 연동성을 확보해야 한다.

**제6장 보칙**

**제28조 (개인정보 보호)**

1. 업무와 관련되어 취득한 개인정보가 포함된 문서는 외부에 유출되지 않도록 시건장치가 있는 문서보관함 또는 보안기능을 갖춘 저장매체에 보관하여야 한다.
2. 회사는 개인정보보호 위하여 그 관리업무를 총괄 담당하는 책임자(이하 “개인정보보호책임자”)를 지정하며, 개인정보보호책임자는 다음 각 호의 업무를 수행한다.
3. 개인정보 보호 계획의 수립 및 시행
4. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
5. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
6. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
7. 개인정보 보호 교육 계획의 수립 및 시행
8. 개인정보파일의 보호 및 관리·감독
9. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무
10. 개인정보보호책임자는 개인정보 관리실태를 점검하기 위하여 각 부서에 불시점검을 실시할 수 있다.
11. 개인정보보호책임자는 전항의 점검결과 보안관리 상태가 불량한 임직원에 대하여는 엄중 문책 또는 경고조치를 하여야 한다.

**부칙**

이 규정은 2019년 1월 20일부터 시행한다.