회승R&A HWASEUNG	기업정보보호 관리규정	문서번호	HSG-001
		개 정 일	3 / 21.03.03
		페 이 지	1 / 19

승 인

작성팀(부서)	기획팀
작 성 자	이 지 학

개정번호	일 자	개 정 내 용	작성	검토	승인
0	09.03.01	- 신 규			
1	11.07.01	- 1차 개정 (정기개정 검토) 규정추가(서약서 징구, 협력업체관리)			
2	12.02.01	- 2차 개정 보안위원회 설립 및 세부규정 추가			
3	21.03.03	- 3차 개정 (정기개정 검토) 문서번호 변경, 정보자산 분류 추가 등			

1. 총칙

1.1 목적

본 규정은 회사의 기업정보 관리 및 보호에 관한 필요한 사항을 정하여 회사의 발전을 도모함을 목적으로 한다.정보보호 활동을 위한 기반 조직을 구성하고, 비 인가자의 부적절한 행위로부터 당사 근무인원 및 시설을 안전하게 보호하는 것과 정보시스템에 의하여 처리, 저장, 소통되는 자료를 바이러스, 해킹 등의 위협으로부터 보호하고 취약요인을 제거하여 회사의 정보보호 관리를 지속적으로 이루어지게 하는 것을 목적으로 한다.

1.2 적용범위

본 규정은 당사의 모든 임직원, 계약관계에 있는 자 및 출입자와 정보자산이 기록, 저장, 활용되는 모든 매체, 전산장비 및 관련시설을 포함한 모든 정보자산에 적용된다. 모든 보안통제는 보안정책서에 근거하여 실시한다.

1.3 정 의

① "기업정보"라 함은 회사가 보유 또는 보유할 정보로서 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로, 상당한 노력에 의하여 비밀로 유지된 생산 방법.판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.

② "관리보안"이라 함은 보안조직 구성 및 운영, 보안정책 및 절차관리, 보안교육, 보안점검, 보안감사, 보안사고 조사 등의 보안활동을 말한다.

③ "물리보안"이라 함은 회사의 시설 및 인원을 보호하기 위한 출입통제, 정보자산의 반 · 출입 통제, CCTV관리 등의 보안활동을 말한다.

④ "기술보안"이라 함은 정보시스템의 보호 및 정보시스템을 통한 유출을 예방하기 위한 운영관리, 정보시스템 접근통제, 개발 및 유지 보수, 침해사고 관리 등의 보안 활동을 말한다.

1.4 보호대상

이 규정은 회사가 보유하고 있는 다음 각호를 그 보호대상으로 한다.

① 기업정보 그 자체 및 기업정보가 화체된 물건
(서류,도면,복사물,이동식저장장치,파일,자재,생산품등)

② 생산설비 및 연구장비 관련 정보

③ 기업정보 통제구역 관련정보 및 기타정보

2. 기업정보 보안조직

2.1 보안조직 구성 및 관리주체

2.1.1 보안업무와 관련된 전사보안조직의 구성 및 관리는 보안위원회에서 주관한다.

2.1.2 보안조직 구성 및 운영에 관한 절차를 마련하고 CISO의 승인을 득한 후 등록 관리한다.

2.1.3 보안에 대한 주요 사항의 결정 및 사내 하부조직까지의 원활한 정책 전달 및 이행을 위해 CISO, 전사보안담당자를 구성원으로 하는 협의체를 구성하고 정기적으로 운영해야 한다.

2.2 보안위원회 업무분장 (책임과 역할)

2.2.1 CISO (Chief Information Security Officer)

① 대표이사의 권한을 위임 받은 임원으로 한다.

② 최고정보보호책임자로서 보안에 관련한 모든 정책을 결정한다.

③ 회사의 보안규정을 수립하고 교육, 공지 등을 활용하여 적용한다.

④ 보안관련 법령 및 관련사의 보안정책 변경 등 외부환경 변화에 따른 회사의 보안정책을 재 검토하고 필요 시 보안규정에 반영하거나 보안교육, 점검, 감사 등의 조치를 시행한다.

⑤ 보안사고 발생 시 외부 수사기관과의 연계여부를 판단하고 대책 수립 및 징계를 시행한다.

⑥ 정보보호 활동 계획 및 예산에 대한 운영 및 승인을 시행한다.

⑦ 분기 1회 이상 정기적으로 팀 보안담당자 회의를 개최하여 보안 정책의 하부조직 전파에 노력한다.

⑧ 전사보안담당자를 선임한다.

⑨ 보안업무를 기획, 시행하도록 전사보안담당자에 지시하고 시행사항을 관리감독 한다.

2.2.3 전사보안담당자

전사보안담당자는 관리보안담당자, 물리보안담당자, 기술보안담당자로 역할을 구분하고, 규정에서 정한 보안업무를 수행한다.

① 전사보안담당자는 CISO가 선임한 자로 한다.

② 보안업무를 CISO에보고, 승인 후 시행한다.

③ 보안교육 및 홍보를 실시한다.

④ 정보자산의 정기적인 점검을 통해 취약성 조사 및 대응방법을 마련하여 보안사고를 사전에 예방한다.

1) 관리보안담당자

① 교육계획을 수립 및 시행하고, 각종 보안 이벤트 시행, 모니터링, 정보자산에 대한 정기적인 점검 등을 통한 보안사고 예방활동을 수행한다.

② 보안사고 발생 시 이에 대한 조사, 조치활동을 담당한다.

2) 물리보안담당자

① 각 팀에서 요청하는 보안구역설정을 검토, 승인하고, 그 결과를 요청부서에 회신하고 이를 현황으로 관리해야 한다.

② 물리보안시스템을 운영하며 관련된 절차를 수립하고, 그 절차에 따라 운영

현황을 관리하며 필요 시 CISO에 보고, 조치한다.

3) 기술보안담당자

① 정보기술 관련한 전 부문의 보안업무를 총괄하여 수립 및 시행한다.

② 보안규정 상의 보안업무 수행사항을 적용 및 실행한다.

③ 정보기술 보안에 관련한 별도의 세부지침을 마련하여 시행한다.

④ 정보기술 보안시스템의 관리 및 성과분석을 실시한다.

⑤ 보안사고 발생 시 기술적인 조사, 조치 등을 지원한다.

4) 팀 보안책임자

각 팀의 팀장으로 해당 팀 내 보안업무를 수행, 조정, 감독한다.

① 팀 내 각종 기업비밀의 보안성 검토 및 보안문서 여부를 결정한다.

② 팀 내 자체 보안점검이 정상적으로 이행되고 있는지 확인하고 감독한다.

③ 팀 내 시건장치 등이 적절히 사용, 관리되고 있는지 확인하고 감독한다.

④ 팀 보안담당자를 임명한다.

⑤ 팀 내 보안사고 발생시 또는 발생할 우려가 있는 경우 CISO에게 통보한다.

⑥ 회사의 보안정책이 효과적으로 이행될 수 있도록 적극 지원한다.

5) 팀 보안담당자

① 팀 보안책임자가 임명한 자로 해당 팀의 전반적인 보안실무관리를 담당하며 전사보안담당자와 긴밀한 협조체계를 구축하여 정보보호 활동에 있어서 부서간 이견 발생시 협의체 역할을 수행한다.

② 보안담당자 회의는 회사의 보안방향 및 정책에 대한 사항의 실무협의, 보완대책 등을 강구하고 임직원에게 전파하는 업무를 수행한다.

2.2.4 보안 침해사고 대응팀

① 침해사고 대응팀은 CISO와 관리 · 물리 · 기술 보안담당자로 구성된다.

② 침해사고 대응팀은 보안사고 발생시, 사고조사의 진행 · 증거자료 확보 · 재발방지 대책 수립등의 대응을 실시한다.

③ 공동작업이 필요하다고 판단되는 사안의 경우, 외부업체 및 대외기관에 통보하고 협조를 요청할 수 있다.

3. 기업정보보호 계획 및 규정

3.1 계획수립

3.1.1 보안위원회는 매년 기업정보보호 계획을 수립한다.

3.1.2 수립된 계획은 경영진에 보고 및 승인을 받도록 한다.

3.1.3 매년 수립된 기업정보보호 계획에 근거하여 정보보호 실적을 관리하도록 한다.

3.2 기업정보보호 관리절차수립 및 개정

3.2.1 보안위원회는 기업정보보호 관리규정을 수립한다.

3.2.2 기업정보보호 관리규정은 매년 1회 개정에 대한 검토를 실시하며, 법령 및 고객사의 정책변경에 따라 관리규정의 개정을 실시 할 수 있다.

3.2.3 기업정보보호 관리규정의 수립 및 개정은 보안위원회의 협의하에 실시토록 하며, 제 · 개정본에 CISO의 승인을 받도록한다.

4. 기업정보의 보호관리

4.1 기업정보구분

4.1.1 기업정보는 그 중요성과 가치의 정도에 따라 일반 · 보안 정보로 구분한다.

4.1.2 일반정보는 대외적으로 노출, 공개되는 경우에도 특별히 문제가 되지 않을 내용으로 공시자료 등 대외 공개를 목적으로 만들어 졌거나, 인터넷 검색 등을 통해 쉽게 취득할 수 있는 자료를 의미한다.

4.1.3 보안정보는 누설될 경우 회사에 손실을 초래하거나, 해로운 결과를 발생시킬 수 있는 자료를 의미한다.

4.2 보안점검 및 보안감사

4.2.1 기업정보의 안전한 관리를 위하여 기업정보를 취급하는 전 부서에 대하여 정기적 보안 점검 및 감사를 실시한다.

4.2.2 기업정보 관리책임자는 회사에서 정한 보안통제가 적절히 이행되는지 확인 함으로써, 잠재적인 정보보안 침해의 가능성과 그로 인한 피해를 최소화 하는데 그 목적이 있다.

4.2.3 보안점검은 연1회 CISO가 지정하는 인원으로 실시한다.

4.2.4 보안점검은 보안정책, 보안조직, 자산관리, 인적보안, 물리적보안, 기술적보안에 관한 사항이 포함된 지표를 통하여 실시한다.

4.2.5 보안점검 실시인원은 점검결과를 CISO에 보고하며, 해당 지적사항 발생 부서는 개선방안 및 개선결과를 CISO에 보고한다.

4.3 기업정보 통제구역 설정

4.3.1 보안위원회는 기업정보의 보호와 중요시설장비 및 자재의 보호를 위하여 필요한 경우 일정한 범위를 통제구역으로 지정한다.

4.3.2 제1항의 통제구역에는 “통제구역"임을 표시하고 관계자 이외의 출입을 통제하며, 출입자 명부를 비치하여 출입자를 기록·보존하여야 하고 필요할 경우 기업정보 준수에 관한 서약서를 징구해야 한다.

4.3.3 통제구역은 보안위원회의 협의와 CISO의 승인을 득한 뒤 지정하도록 한다. 통제구역 해지절차도 이와 같다.

4.3.4 통제구역은 허가된 인원에 한하여 출입할 수 있도록 보안장치를 설치한다.

4.4 외부인 접근통제

4.4.1 회사의 출입구에 경비인력 및 보안장비(CCTV, 차단기 등)을 설치하여 미허가자의 출입을 제한한다.

4.4.2 방문자는 절차에 따라 방문자의 신상 및 방문 목적을 방문일지작성·방문증 수령 후 출입하도록한다.

4.4.3 회사내의 방문 및 면회자 발생시, 해당 직원의 인솔하에 출입한다.

4.4.4 회사 경비 인력은 전산장비(노트북, PC, USB, 하드디스크)의 반·출입 시 출입자에게 해당 사항을 기재토록하고 당해 기록을 관리하도록 한다.

4.4.5 경비인력은 차량출입을 통제하며, 차량 출입시 당해 기록을 출입일지에 기록·보관 하도록 한다.

4.5 전산장비 운영관리

4.5.1 개인용 전산장비는 로그인 및 화면보호기 비밀번호(영숫자혼용 6자리이상)가 설정되어 있어야 한다.

4.5.2 모든 PC는 악성코드 실행방지 솔루션 등 보안시스템이 설치되어야 하며, 사용자는 최신업데이트 및 최신보안패치를 적용해야 한다.

4.5.3 재해발생시 정보자산의 보호를 위하여 재해복구계획을 수립하여야 하며, 이에 따른 모의훈련을 실시하여야 한다.

4.5.4 PC내의 파일을 공유할 필요가 있을 경우, 비밀번호가 설정된 공유폴더를 설정하여, 인가된 사용자만 접근할 수 있도록 한다.

4.6 정보침해관리

4.6.1 정보침해사고 발생시 보안사고에 효과적인 대응을 위하여 본조 2.2.4의 보안 침해사고 대응팀을 구성하도록 한다.

4.6.2 정보침해사고 발생시 보안 침해사고 대응팀은 보안사고증거를 수집 및 관리하며 보안사고에 대한 조사내용을 기록하고 그 내용을 CISO에게 보고하여야 한다.

5. 사원의 기업정보 보호의무

5.1 채용시

신규로 채용된 사원은 보안서약서(별지 #1)를 작성하여 인사팀에 제출한다.

5.2 재직중 기업정보누설 금지

5.2.1 사원은 재직시 취득한 기업정보에 대하여는 이 절차에 따라 취급 · 관리해야 하며 허가없이 이를 유출 · 공개 또는 사용할 수 없다.

5.2.2 연구개발 결과, 신제품 등을 발표하거나 전람회 등에 출품하여 부득이하게 기업정보를 공개하게 되는 경우에는 사전에 승인을 얻어야 한다.

5.3 퇴직시

5.3.1 회사의 사원이었던 자는 회사의 사전승인없이 재직시 취득한 기업정보를 공개 · 유출 또는 사용할 수 없다.

5.3.2 사원이 퇴직할 경우 그 사원이 보유하고 있는 모든 기업정보를 반납받고 퇴직자 기업정보유지 서약서(별지 #2)를 작성하여 제출하도록 한다.

5.3.3 퇴사자 발생 즉시 인사팀은 퇴직사항을 전산팀에 통보하며, 전산팀은 퇴직자의 정보접근 권한을 24시간 이내에 삭제하여 인사팀에 통보한다.

5.3.4 퇴직한 사원이 동종의 경쟁업체에 취업한 경우 별도 서식의 통지서 (별지 #3)를 해당 경쟁업체에 송부한다.

6. 기업정보의 생성과 취득

6.1 기업정보의 창출 및 귀속

사원이 직무와 관련하여 연구 · 개발한 기업정보는 회사에 귀속한다. 다만, 자신의 일반적 지식, 경험, 기술에 근거하여 창출한 기업정보는 특별한 약정이 있을 경우 그 약정에 따르고, 약정이 없을 경우 당해 사원의 귀속으로 한다.

6.2 기업정보 신고

6.2.1 사원이 재직 중 기업정보를 창출한 경우, 팀 보안책임자에게 신고한다.

6.2.2 사원이 본 절차의 적용을 받지 않는 타인과 공동으로 회사의 업무와 관련된 기업정보를 창출한 경우에도 6.2.1의 규정에 따라 신고한다.

6.3 보상

사원이 창출한 기업정보 중 상당한 가치가 있을 경우 보상금을 지급할 수있다.

6.4 취득

사원이 기업정보를 외부로부터 취득했을 때, 본 규정 6.2 기업정보 신고 조항을 준용한다.

7. 기업정보의 사용

7.1 사용

회사의 기업정보는 CISO의 승인을 얻어 사용할 수 있다.

7.2 양도

7.2.1 기업정보를 양도할 때에는 관련부서와 협의를 하고 CISO의 승인을 얻어야 한다.

7.2.2 회사는 기업정보를 양도한 후에도 필요에 따라 관계기록을 폐기하지 않고 기업정보 유지 · 관리를 수행해야 한다.

7.3 부서간 사용

7.3.1 타부서 관리의 기업정보는 일정한 절차에 따라 이용할 수 있다.

7.3.2 부서간 기업정보를 사용·대여할 때에는 부서 책임자간에 인계인수 절차를 거쳐야 하며, 반환하는 때에는 또한 같다.

7.4 이송

7.4.1 기업정보를 사내에서 대여·사용·유통을 위하여 이송할 때에는 밀폐 포장이나 용기 등을 사용하여야 한다.

7.4.2 부득이 기업정보를 통신수단에 의하여 이송할 때에는 음어를 사용하거나 주요내용 부분은 분리하여 이송하여야 한다.

7.5 폐기

더 이상 활용가치가 없는 기업정보는 일정한 절차에 의해 폐기할 수 있으며, 폐기 후에도 필요한 경우에는 계속하여 보호·관리한다.

8. 협력업체등에 대한 비밀관리

8.1 협력업체 및 외주업체

기업정보보호를 위하여 협력업체(별지 #4) 및 외주업체(별지 #5)로 하여금 보안서약서를 작성하여 제출하도록 한다.

8.2 외부와 공동 프로젝트 수행

회사가 외부 연구기관 등에 연구개발 프로젝트를 의뢰할 경우, 외부 연구기관 및 개발에 참여하는 연구기관 소속직원에게는 기업정보보호 서약서(별지 #6)를 작성 · 제출하도록 한다.

9. 기업정보 침해구제

9.1 구제조치

기업정보를 침해당했을 때에는 지체없이 관계법령에 의한 필요한 구제조치를 취하여야 한다.

9.2 보안위반 조치

9.2.1 위반사항의 경중을 판단하여, 경미한 위반의 경우 전사보안담당자 명의의 주의조치를 해당 직원 및 소속 팀장에 통보하며, 중요한 위반이라고 판단되는 경우 CISO에 보고 후 규정에 따라 조치한다.

9.2.2 기업정보누설자에 대해서는 9.1의 규정에 의한 조치와 동시에 별도로 사규(HM 310, 인사관리절차)에 따라 징계할 수 있다.

9.2.3 유사사고 재발방지를 위해 대책을 수립, 시행하고, 징계 결과는 임직원 전원에게 공지한다

9.3 임직원

9.3.1 기업정보보안 관리규정 및 관련 지침/절차를 위반한 사실을 인지하는 경우 전사보안담당자에 즉시 위반 사실을 통보해야 한다.

9.3.2 본인의 실수 또는 의도하지 않게 정보가 노출, 제공되었음을 확인하는 경우 전사보안담당자에 관련사실을 통보해야 한다.

9.4 경미한 위반

9.4.1 실수 또는 과실에 의한 단순한 규칙/지침 위반이라고 인정되는 경우

9.4.2 위반이력이 없는 임직원이 규정, 절차 등의 미 인지로 규칙/지침을 위반한 경우 중 중대한 위반의 사유가 되지 않는 경우

9.4.3 본인의 위반사실을 통보해온 경우 중 중대한 위반 사유가 되지 않는 경우

9.4.4 위반 회수에 따라 다음과 같이 조치를 상향 한다

① 1회 위반 : 당사자 구두 경고

② 2회 위반 : 당사자 서면 경고(시말서) 및 팀장 구두경고

③ 3회 위반 : 당사자 및 팀장 서면 경고(시말서)

④ 4회 이상 : 고의적 정책 미 준수로 중대한 위반으로 상향

9.5 중대한 위반

9.5.1 인사위원회에 회부하여 경고 이상의 징계를 시행한다.

9.5.2 고의로 보안 규정, 절차, 지침을 우회하는 행위를 한 경우

9.5.3 보안사고와 직, 간접적으로 관련된 사안으로 인정되는 경우

9.5.4 중대한 과실이거나, 동일한 위반을 반복적으로 지적 받는 경우

10. 정보자산 분류

10.1 분류주체 및 주기

10.1.1 팀보안책임자는 회사의 자산분류 기준을 이해하고, 이를 바탕으로 정보의 생성자(문서작성자)가 최초분류를 시행하도록 공지, 점검 한다.

10.1.2 임직원은 문서를 생성할 때 분류기준에 따라 등급을 구분하여 회사 보안정책이 준수되도록 분류기준을 인지하고, 항상 분류된 상태로 문서를 관리 한다.

10.1.3 팀보안담당자는 팀 내 업무 변동사항 발생 시 2주 이내, 특별한 변동 사항이 없는 경우에도 6개월에 1회 정기적으로 검토/조정을 시행 한다.

10.1.4 등급이 분류된 정보자산은 인식할 수 있는 관리자, 자산번호, 보관위치 등을 확인 할 수 있는 인덱스를 부착하여 관리해야 한다.

10.2 정보자산의 구분

10.2.1 정보자산은 '비밀(Secret)', '대외비(Restricted)', '공개(Public)'로 등급을 구분 한다.

10.2.2 비밀, 대외비는 당사 영업비밀로 구분되며 '11.영업비밀관리기준' 및 관련 규정을 준수해야 하며, 공개 등급의 문서는 관리 대상에서 제외한다.

10.2.3 대외비는 모든 임직원이 사용할 수 있으나, 사외에 노출되는 경우 회사에 손해를 끼치거나 해로운 결과를 초래할 우려가 있는 자료를 말한다.

10.2.4 비밀 등급은 업무상 관련 있는 임직원만 제한적으로 사용이 허용되는 자료로, 사외로 노출되는 경우 회사에 상당한 손실을 초래하거나, 회사 사업계획의 폐기, 수정, 영업손실 등을 초래할 우려가 있는 자료를 말한다.

10.2.5 공개 등급은 대외로 노출, 공개되는 경우도 특별히 문제가 되지 않을 내용으로 공시자료 등 대외 공개를 목적으로 만들어 졌거나. 인터넷 검색 등을 통해 쉽게 취득할 수 있는 자료를 말한다.

10.2.6 임직원(계약관계에 있는 자 포함)에 의해 작성된 모든 문서는 재 분류 전까지 대외비로 취급하며, 관련 규정을 준수 하여야 한다.

10.2.7 보안등급의 추가 지정이 필요한 경우 CISO의 승인을 얻어 '극비' 등급을 지정, 사용할 수 있다.

10.2.8 외부 반입 문서의 등급 분류 기준을 수립하여, 전사보안담당자의 승인을 득한 후 운영해야 한다.

10.3 정보자산의 관리

10.3.1 전사보안담당자는 팀 단위에서 작성할 수 있는 정보자산분류기준 (템플릿)을 제공해야 한다.

10.3.2 전사 보안주관부서는 1년에 1회 이상 팀별로 파악된 정보자산의 리스트를 총괄 취합/관리하며, 과소, 과도 분류가 되지 않았는지 유효성 검증을 실시해야 한다.

11. 영업비밀관리기준

11.1 영업비밀의 보관 및 관리

11.1.1 영업비밀은 생성시 원본 문서에 해당 등급을 표기해야 하며, 생성과정에 있는 중간산출물 및 해당내용의 일부를 사용한 문서도 동일한 방법으로 관리되어야 한다. 기 생성된 문서 중 보안등급이 구분되지 않는 문서의 경우 소급하여 등급 분류를 시행한다.

11.1.2 출력된 영업비밀에는 그 등급이 매 페이지마다 쉽게 식별 가능하도록 표기 되어야 하며, 출력 시 표기하지 못한 문서의 경우 출력 후 고무인 등을 활용하여 표기한다.

11.1.3 출력된 영업비밀은 개방된 장소에 보관해서는 안되며, 시건 장치가 있는 장소에 보관하고 팀보안책임자가 지정하는 자가 관리한다.

11.1.4 출력된 영업비밀은 보존기간이 만료되면 1개월 이내에 복원할 수 없는 형태로 파기 한다. 단, 업무적 이유로 파기를 유예할 필요가 있는 경우 목적과 유예기간 등을 서면으로 전사보안담당자에 보고 후 보관한다.

11.1.5 영업비밀이 휴지통, 공용 회의실 등 직원이 통제할 수 없는 장소에 방치된 경우 문서의 출력자, 해당 팀장을 보안규정위반으로 조치 한다.

11.2 영업비밀의 이관

11.2.1 보직 변동으로 해당 영업비밀을 소유할 필요가 없는 경우 전보자는 '업무인수인계서'에 취급 영업비밀의 인수인계 내용을 작성하고, 전자문서 및 출력문서 등 모든 종류의 영업비밀을 인수자에 인계한다.

11.2.2 팀보안책임자는 인계/인수 절차에 따라 영업비밀이 적절히 이관되었는지 확인하고 인계자 소유하고 있는 영업비밀이 모두 파기 되었는지 확인한다.

11.2.3 업무상 이유로 기존 영업비밀의 일부를 전보된 부서에서 사용할 필요가 있는 경우 그 목적과 파일의 목록을 이전 팀보안책임자에 서면으로 보고 후 활용할 수 있다. 서면보고과정 없이 보유하는 경우 이유를 막론하고 고의적인 정보취득으로 보안위반자 처리규정에 따라 조치 한다.

11.3 영업비밀의 배포 및 반출

11.3.1 영업비밀을 본인의 업무와 직접적으로 관련이 없는 곳으로 반출할 사유가 발생하거나 국가기관 등 외부에서 요청한 자료의 범위에 영업비밀이 포함되는 경우 전사보안담당자의 사전 승인을 얻어 반출한다.

11.3.2 본인의 업무 수행을 위해, 사외 반출하는 경우 반출처와 반출일시, 반출 내역을 회사가 정한 양식에 따라 작성하여, 주간 단위로 팀보안책임자에 보고하고, 결재를 받아 보관한다. 단, 기술자료(도면)를 배포/접수 할 수 있는 시스템이 구축된 경우 별도의 기록을 작성하지 않고 시스템 로그로 대체한다.

11.3.3 영업비밀의 반출 이력은 2년 이상 보관되어야 하며, 필요 시 쉽게 조회 가능한 상태로 관리되어야 한다. 사내 배포의 경우 영업비밀의 소유권자(작성자)의 판단에 따라 회사가 정하는 보호조치가 적용된 상태로 필요한 인원에 한정하여 배포한다.

11.3.4 본인이 작성한 영업비밀이 아닌 경우 배포, 반출할 수 없으며, 작성자의 승인을 얻거나 작성자에 반출, 재 배포를 요청해야 한다.

11.4 영업비밀의 파기

11.4.1 전자문서 형태의 영업비밀은 회사가 정하는 소프트웨어를 활용하여 복원 불가한 상태로 파기 해야 하며, 사본도 같은 방법으로 파기 한다.

11.4.2 전자문서 이외의 영업비밀은 문서세단기를 사용하여 원형을 확인 할 수 없는 상태로 파기해야 한다. 임직원이 사용할 수 있는 문서세단기가 설치되지 않은 경우 전사보안담당자는 별도의 파기절차를 수립하여 운영해야 한다.

11.4.3 전자문서 파기용 소프트웨어를 지정, 공지 하지 않은 경우 파기에 대한 책임은 전사보안담당자에 있다.

12. 보 칙

12.1 교육

12.1.1 기업정보취급인가자는 관련 교육을 정기적으로 이수하여야 한다.

12.1.2 신규 및 재직 사원에 대해서도 정기적으로 기업정보보호에 관한 보안 교육을 연 2회 이상 실시하여야 한다.

12.2 벌칙

사원이 본 절차를 위반했을 시, 관계법령에 의한 민·형사 책임과는 별도로 사규(HM310, 인사관리절차)에 의하여 징계를 받을 수 있다.

13. 기 타

13.1 관련 문서

· 인사관리절차 (HM 310)

[별지 제1호 서식]

보안서약서 (신규입사 및 재직자 용)

본인은 회사 재직 중 및 퇴직 후 2년 간은 화승그룹의 보안규정을 충분히 숙지하여 업무상 비밀을 제3자에게 공개하거나 누설하지 아니하고, 창업이나 경쟁관계에 있는 회사 및 기타 제3자를 위하여 절대 사용하지 않음은 물론 업무상 비밀과 관련된 경쟁업체에 겸직하거나 그곳으로 전직하거나 그 업체와 동업을 하지 않을 것을 약속하면서 다음과 같이 서약합니다.

1. 회사로부터 취득한 정보 또는 회사의 업무와 관련하여 취득한 모든 정보는 회사 본인의 업무에 한해 이용하며 화승그룹의 보안규정을 준수한다.

2. 회사의 구성원으로서 회사의 지적재산권을 보호하고, 아래와 같은 업무 수행과정에서 획득한 영업비밀 및 고객정보에 대한 보호의무를 준수한다.
   (1) 사업계획, 연구개발계획에 관한 비밀사항
   (2) 개발, 사업 프로젝트 등에 관한 비밀사항
   (3) 타사 제휴 현황에 관한 비밀사항
   (4) 생산방법, 생산조건, 공정기술, 장치 등 기술비밀에 관한 사항
   (5) 판매방법, 고객명부 등 영업비밀에 관한 사항
   (6) 자회사, 협력업체 등 사업파트너와의 사업정보에 관한 비밀사항
   (7) 기타 회사에서 영업비밀로 취급, 관리하는 사항

3. 제3자의 지적재산권과 영업권을 보호함으로써 회사의 이미지를 실추시키지 아니하고 그와 관련하여 회사에 금전적 손해를 끼치지 아니한다.

4. 업무상 허가 받지 않은 정보나 시설에 접근하지 않으며, 업무 이외의 용도로 회사 보유 자산을 사용하지 아니하고, 회사 시설 내에도 무단으로 접근하지 아니한다. 또한 회사 시설 내에 사적 정보 및 제3자의 지적재산권이나 영업비밀에 관한 내용을 보관하지 아니한다.

5. 회사에서 제공하는 PC, 메일, 메신저, 보안S/W 및 기타 장비 사용에 대한 이력점검 및 보안감사에 동의하며 적극 협조한다.

6. 회사의 구성원으로서 인적자원관리상 개인정보제공이 필요한 부분에 대해서 개인정보보호법 등 규정에 따라 개인정보를 수집·이용하는 것에 동의한다.

7. 퇴직 시 회사의 지적재산 및 영업비밀 등 보안이 요구되는 사항에 관하여 퇴직 후 2년 간 비밀유지를 하는 비밀준수서약서를 제출한다.

8. 경력사원 입사의 경우 경업금지 관련 전 직장의 자료를 업무시 활용하지 않는다.

9. 이외 사항에 대해서는 보안규정의 내용에 동의하고 준수할 것을 약속한다.

본인은 위의 사항을 숙지하고 이를 성실히 준수할 것이며, 만일 이를 위반하였을 경우 관련 법령 및 회사 규정에 따라 민.형사상의 책임을 지고, 손해액을 지체없이 변상할 것을 서약합니다.

년 월 일

서 약 자 : (인)

주식회사 화승R&A 귀중

[별지 제2호 서식]

퇴직자 기업정보유지 서약서 (퇴직자용)

본인은 퇴직 후 화승R&A의 기업정보에 대하여 다음과 같은 사항을 준수할 것을 서약합니다.

1. 본인은 재직기간 중 지득한 회사의 기업정보를 퇴직 후 회사의 의사에 반하여 사용하거나 공개 또는 누설하지 아니한다.

2. 본인은 퇴직일로부터 3년간 재직시 지득한 기업정보를 이용하여 창업하거나 경쟁사에 취업하지 아니한다.

3. 본인은 회사의 기업정보와 관련하여 입수한 모든 자료를 퇴직시까지 반납한다.

4. 기타 회사의 기업정보를 준수하기 위하여 성실한 노력을 다한다.

이상과 같이 서약하며 상기 사항을 위반하여 귀사에 손해를 끼칠 경우 민·형사상의 모든 책임을 감수할 것입니다.

년 월 일

소 속 :

성 명 : (인)

[별지 제3호 서식]

통 지 서 (퇴직 임직원 타기업 취업시)

0 0 0 주식회사

대표이사 0 0 0 귀하

귀사의 무궁한 발전을 기원합니다.

귀사에 취업한 (성명:), (주민번호:),

(주소:)은 저희 회사 재직중

(~ 간) □□□ 개발 및 기업정보관리 업무에 종사하였고, 이와 관련한 저희 회사의 기업정보를 보유하고 있으며, 저희 회사에서는 위의 사람에게 기업정보유지 서약서를 제출받은 바 있습니다.

따라서, 귀사에서 위의 사람이 저희 회사에서 하던 업무와 동종의 업무에 종사하게 되면 저희 회사의 기업정보를 침해할 우려가 있음을 알려드리오니 부디 저희 회사의 기업정보를 침해하는 일이 없도록 주의하여 주시도록 통지하여 드립니다.

년 월 일

화승R&A 대표이사 ○○○

[별지 제4호 서식]

보안 서약서 (협력업체에 대한 기업정보 제공시)

성　　명 :

주민등록번호 :

주　　소 :

1. 본인은 이번 기업정보에 관한 정보자료를 지득 또는 제공받음에 있어서 본 기업정보 뿐만 아니라 본 기업정보로 인하여 알 수 있는 모든 기업정보를 누구에게도 공개 · 누설하지 않을 것을 서약합니다.

2. 본 기업정보가 귀사에 의해 적법하게 공개된 경우에도 미공개 부분에 대해서는 제1항과 같은 비밀유지 의무를 부담할 것을 서약합니다

3. 본 기업정보를 사용한 후에는 즉시 본 기업정보를 귀사에 전부 반환하며 제 1항과 같은 비밀유지 의무를 부담할 것을 서약합니다.

년　　월　　일

서약인　　인

화승 R&A 귀중

[별지 제5호 서식]

정보보호 서약서 (사내 외주 · 용역업체 용)

본인은 주식회사 화승R&A(이하 '회사'라 함)의 사내 외주업체 임·직원으로서 기업정보의 보호와 관련하여 다음과 같이 서약합니다.

1. 본인은 회사 재직중, 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로써, 상당한 노력에 의하여 비밀로 유지된 회사의 생산방법, 판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보(이하 '영업비밀'이라함)의 보호와 관련된 회사의 각종 규정을 준수하겠습니다.

2. 본인은 업무수행중 또는 업무와 관련없이 취득하게 되는 다음과 같은 사항 및 기타 영업비밀을 지정된 업무에 사용하는 경우를 제외하고는 어떠한 방법으로도 회사 내외의 제3자에게 누설하거나 공개하지 않겠습니다.
(다만, 회사의 사전 서명동의가 있거나 영업비밀보호관련 규정에 의해 허용된 경우는 예외로 함.)

(1) 인사, 조직 및 재무현황, 생산.판매현황, 마케팅 기법 등 경영상의 정보
(2) 제품의 설계방법, 설계도면, 제조공정, 제조장치, 제조와 관련된 기술상의 정보
(3) 제품의 연구개발(R&D)계획, 작업보고서, 및 일지의 내용, 실행데이터, 연구성과 분석자료 등 연구개발에 관한 정보

3. 본인은 허가 받지 않은 정보나 시설 등에는 절대로 접근하지 안고 회사의 보안규정 및 정책을 반드시 준수할 것이며, 특히 E-mail사용과 관련하여 회사에 손해를 입힐 수 있는 기술 및 경영정보의 유출을 방지하기 위한 회사의 적법한 메일통제 정책에 동의합니다.

4. 본인은 업무수행중 또는 업무관련 없이 취득한 기업정보에 대하여 지정된 업무에 대하여 지정된 업무에 사용하기 위한 목적 외의 복사, 녹음 및 기타 방법에 의한 복제를 일절 하지 않겠습니다.

5. 본인은 본인의 퇴직시 본인이 관리하고 있던 도표, 설계도, 명세서, 메모, 보고서, 노트, 자기테이프, 디스크, 파일, 기타 기록매체 등 기업정보와 관련된 사항이 들어있는 일체의 자료를 회사에 반납하고, 이에 관해 어떠한 형태의 사본도 개인적으로 보유하지 않겠습니다.

6. 본인은 위 각 서약사항 위반 시, [부정경쟁방지 및 영업비밀보호에 관한 법률]에 규정된 민·형사상 책임, 민법상의 채무불이행 또는 불법행위로 인한 손해배상 책임, 형법상의 업무상 배임 등의 책임, 기타 제반 민,형사상의 책임을 지는 것은 물론 회사의 금전적 손해에 대해 손해액 일체를 즉시 배상하도록 하겠습니다.

서명에 앞서 위 서약사항을 세심히 읽어보았음을 확인합니다.

년 월 일

소 속 :

성 명 : (인)

[별지 제6호 서식]

기업정보보호 서약서 (공동연구 프로젝트 진행시)

본인은 이번 귀사의 000 연구프로젝트에 그 일원으로 참여하게 되었으며 이에 같은 사항을 준수할 것을 서약합니다.

1. 본 프로젝트 추진의 사실, 그 성과 및 본 프로젝트를 수행하는 과정에서 알 수 있는 귀사의 기업정보를 유지하고 회사 밖은 물론 귀사의 종업원이라고 하여도 프로젝트에 직접 관여하지 않는 자에 대해서는 이것을 공개 또는 누설하지 않을 것을 서약합니다.

2. 본 프로젝트 추진의 사실 및 그 성과가 귀사에 의하여 적법하게 공개된 경우라고 하여도 미공개 부문에 대해서는 앞에서와 같은 비밀유지의무를 부담할 것을 서약합니다.

3. 본 프로젝트가 완료된 경우 및 프로젝트 진행중에 어떠한 사유로든 본인이 본 프로젝트를 수행할 수 없게 된 경우, 그 시점에서 본인이 보유하고 있는 모든 기업정보를 포함한 관련 자료를 즉시 귀사에 반납하며 앞에서와 같은 비밀유지 의무를 부담할 것을 서약합니다.

4. 본 프로젝트 추진의 사실, 그 성과 및 본 프로젝트를 수행하는 과정에서 알 수 있었던 귀사의 기업정보를 재직중은 물론 퇴직후에도 5년간 자신을 위해 또는 귀사와 경업하는 사업자 그외 제3자를 위해 사용하지 않을 것을 서약합니다.

주 소 :

주민번호 :

성 명 : (서명)

화승 R&A 귀중