DOC-POL-001

**정보보호 정책서**

개정번호 : 1.00

**㈜1 Shop**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **개 정 이 력** | | | | | | |
| **문서명** | | 정보보호 정책서 | | | | |
| **생성일** | | 2018.10.01 | **보안등급** | | 대외비 | |
| **소유자** | | ㈜1 Shop | **사용자(범위)** | |  | |
| **차수** | **Version** | **개정내용** | | **개정일자** | | **작성자** |
| 1 | 1.00 | 최초 작성 | | 2018.10.01 | | 최유진 |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |

**목 차**

[정보보호 및 개인정보보호 선언 4](#_Toc381270285)

[제1장 개 요 5](#_Toc381270286)

[제1조 목적 5](#_Toc381270287)

[제2조 보호대상 정보자산 5](#_Toc381270288)

[제2장 임직원의 책임과 의무 5](#_Toc381270289)

[제3조 임직원의 책임과 의무 5](#_Toc381270290)

[제3장 정보보호조직체계 6](#_Toc381270291)

[제4조 정보보호 및 개인정보보호 조직 6](#_Toc381270292)

[제5조 정보보호주관부서 6](#_Toc381270293)

[제4장 정보보호 규정체계 6](#_Toc381270294)

[제6조 정보보호 및 개인정보보호 규정체계 6](#_Toc381270295)

[제7조 규정접근의 용이성 7](#_Toc381270296)

[제8조 규정의 공표 7](#_Toc381270297)

[제5장 검토 및 이행 점검 7](#_Toc381270298)

[제9조 정책·지침의 검토 7](#_Toc381270299)

[제10조 정책·지침의 이행점검 8](#_Toc381270300)

[제6장 감사 및 징계 8](#_Toc381270301)

[제11조 보안 감사 8](#_Toc381270302)

[제12조 징계 9](#_Toc381270303)

정보보호 및 개인정보보호 선언

정보시스템과 정보는 ㈜1 Shop(이하 “회사”라 함)의 주요한 자산이며, 이의 신뢰 있는 제공 없이는 직무를 효율적으로 수행하기 어렵다. 그러므로 회사의 경영진은 회사의 정보시스템과 정보를 보호∙ 향상시킬 의무가 있으며, 이는 정보시스템과 정보가 오류, 파괴, 테러, 개인정보 유출, 서비스 중단, 자연재해 등과 같은 여러 종류의 위협으로부터 보호되도록 적절한 조치를 반드시 취하여 한다는 것을 의미한다.

회사는 앞으로의 정보시스템 구축 및 향후 운영 또는 관리 시 예상되는 다양한 보안상의 문제들을 유념하고 이에 대비하여야 한다. 이는 회사의 정보시스템에 대한 해킹, 불법적인 정보 유출 및 접근, 빠르고 광범위한 악성 컴퓨터 바이러스 감염, 그리고 그 외 각종 운영, 실행, 관리상의 문제들이 예상되기 때문이다. 따라서 이로 인한 중요 정보의 손실과 그에 따른 업무의 지연 및 저하, 이로 인한 각종 법적, 사회적, 윤리적인 여파를 철저히 고려하여 이에 따른 적절한 대비책을 마련해야 될 필요성이 날로 증대하고 있다.

그러므로 회사의 정보는 민감성, 가치, 심각도에 준하여 반드시 보호되어야 하며, 정보가 저장되는 매체, 처리되는 시스템, 전송수단에 모두 보안 대책이 적용되어야 한다. 이러한 보호는 직무 수행에 반드시 필요한 정보로의 접근만 허용하는 것을 포함한다. 관리자는 정보가 적절히 보호되기 위한 충분한 시간과 자원을 지원하여야 하며 정보시스템과 정보에 대한 보안 대책이 불충분하다고 판명될 경우에는 신속히 보완 대책을 강구∙시행하여 정보의 노출을 최소화하여야 한다.

회사의 정보보호를 달성하기 위해서는 회사 구성원 모두의 참여와 협조가 요구되며 이를 뒷받침 할 충분한 교육과 참고자료가 제공되어야 한다. 회사의 정보시스템 보호를 수행하는데 필요한 지침과 절차서의 수립 및 제정을 포함한 모든 활동은 정보보호를 담당하는 부서를 중심으로 이루어져야 한다. 끝으로 정보시스템 보안 감사가 주기적으로 전사적으로 행하여져 정보보호가 제대로 이루어지는가를 확인하여야 한다.

**㈜1 Shop 대표이사(Chief Executive Officer) 나 최 고**

개 요

1. 목적

본 정책은 ㈜S-Book RR(이하 ‘회사’라고 한다)의 정보보호에 대한 모든 원칙을 규정하고 이에 따른 인력 및 조직의 역할과 책임을 명시하여 관련 법률 및 규칙 등을 준수함과 동시에 안정적인 업무활동을 보장함을 그 목적으로 한다.

1. 보호대상 정보자산

회사는 다음과 같은 자산을 보호해야 할 정보 자산으로 선언한다.

1. 고객 개인정보
2. 서비스 운영을 통해 수집 및 생성된 정보
3. 회사의 업무수행 과정에서 수집 및 생성한 중요 경영정보
4. 서비스의 제공을 위한 서버/네트워크 등 IT 인프라
5. 사업 수행에 필요한 물리적 업무 환경

임직원의 책임과 의무

1. 임직원의 책임과 의무
2. 모든 임직원은 업무 수행에 있어 신의성실의 원칙에 따라 다른 임직원, 협력업체, 고객의 신뢰에 반하지 않도록 행동한다.
3. 모든 임직원은 회사가 정한 정보보호 정책서, 지침서, 절차서와 그에 상응하는 기준을 반드시 숙지하고 이를 준수한다.
4. 모든 임직원은 본인 및 타 임직원의 위법‧위규 행위가 발생하였거나 발생 가능성이 있는 경우 이를 회사에 알리고 회사가 수립한 관리체계가 지속적으로 유지되도록 노력한다.

정보보호조직체계

1. 정보보호 및 개인정보보호 조직

회사의 정보보호 및 개인정보보호 조직이 구성되어야 한다. (“DOC-POL-002\_정보보호 및 개인정보보호 업무지침” 제6조 3항 참고)

1. 정보보호주관부서

회사의 정보보호 주관부서는 인프라 본부이며, 정보보호최고책임자, 정보보호 관리자, 정보보호 담당자로 구성한다.

정보보호 규정체계

1. 정보보호 및 개인정보보호 규정체계
2. 회사의 모든 임직원이 준수해야 할 정보보호 및 개인정보보호 규정체계는 정책, 지침으로 구성되며 업무의 필요에 따라 매뉴얼을 구비할 수 있다.
3. 회사의 경영방침 및 정보보호 목표를 담고 있는 최상위 정책 문서인 정보보호 및 개인정보보호 정책서, 이를 기반으로 업무 영역별로 정보보호 원칙을 제시한 지침서 등으로 구성된다.
4. 회사의 정보보호 및 개인정보보호 지침은 다음과 같이 구성된다.
5. 정보보호 및 개인정보보호 정책서
6. 임직원을 위한 생활보안지침
7. 서비스 기획자, 개발자, 운영자를 위한 개발보안지침
8. 인프라 운영자, DB 관리자를 위한 IT인프라 보안지침
9. 정보보호 및 개인정보보호 담당자를 위한 정보보호 및 개인정보보호 업무 지침
10. 규정접근의 용이성
11. 회사 정보보호 및 개인정보보호 정책 문서의 운영 관리는 정보보호, 개인정보보호 주관부서에서 담당한다.
12. 정보보호 및 개인정보보호 규정은 회사 임직원 모두가 이해하기 쉽도록 작성되어야 하며, 언제든지 업무에 즉시 참조할 수 있도록 접근성이 보장되어야 한다.
13. 이를 위해 정보보호 및 개인정보보호 지침서가 회사 임직원의 직무에 따라 쉽게 접근하여 참조할 수 있도록 제6조에서 선언한 5개의 규정으로 구성하여 배포한다.
14. 규정의 공표

정보보호 정책 및 지침의 제∙개정 시 임직원이 쉽게 인지할 수 있도록 사내 게시판, 교육 등을 통하여 공표하여야 하며, 정보보호 정책 및 지침의 제∙개정에 대한 이력을 관리하여야 한다.

검토 및 이행 점검

1. 정책·지침의 검토
2. 정보보호 및 개인정보보호 규정은 회사 경영 방침의 변경, 핵심 서비스의 중대한 변경, 신규 보안위협 및 취약점 발생 등에 따라 회사 정보보호 및 개인정보보호 주관부서를 중심으로 신속하게 재검토가 이루어져야 한다.
3. 회사의 정보보호 및 개인정보보호 주관부서는 정기적으로 각 규정을 재검토하고, 회사 서비스 제공에 중대한 영향을 미치는 긴급한 사항이 발생할 경우 즉시 검토하여 해당 내용을 반영하여야 한다.
4. 정책·지침의 이행점검
5. 회사 내 모든 업무 활동은 관련 법률 및 회사 경영 방침을 반영한 회사 정보보호 규정 및 개인정보보호규정에 따라 이루어져야 하며, 궁극적으로 회사 내 정보보호 및 개인정보보호 문화로 정착되어야 한다.
6. 회사 정보보호, 개인정보보호 주관부서는 회사 내 업무 수행 시 정보보호 및 개인정보보호 규정을 준수하고 있는지 여부를 정기 또는 비정기적으로 점검을 실시하여야 한다.

감사 및 징계

1. 보안 감사
2. 보안감사는 정기적으로 수행하는 정기 보안감사와 비정기적으로 수행하는 수시 보안감사, 특별 보안감사로 구분하여 실시한다.
3. 정기 보안감사는 연간 보안감사 계획에 따라 실시하는 계획된 감사를 말하며 기본적으로 연 1회 실시한다.
4. 특별 보안감사는 정보보호 사고의 징후가 있어 확인이 필요한 경우 또는 정보보호 사고 발생 시 실시한다.
5. 수시 보안감사는 정보보호 관련 활동 및 업무 중요도를 고려하여 수시로 해당 업무의 일부 또는 전반에 대하여 보안감사가 필요하다고 인정되는 경우 정기감사와는 별도로 실시 할 수 있다.
6. 징계
7. 정보보호 정책 위반자에 대한 징계는 정보보호위원회의 승인을 거쳐 정보보호 관리자가 인사 관리자에게 요청한다.
8. 인사 관리자에게 요청사항을 인계 받은 인사 담당자는 회사의 인사관리규정에 따라 요청 내역을 처리한다.
9. 임직원은 정보보호 관련 법률과 회사의 정보보호 정책 및 지침을 준수하여야 한다.
10. 정보보호 관련 법률과 정보보호 정책 및 지침에서 규제하는 사항으로서 징계의 대상이 될 수 있는 임직원과 외부인의 정보보호 위반 사항은 다음과 같다.
11. 침해
12. 중요 보안 구역의 물리적 침입
13. 외부 서비스 시스템 가용성 침해 (사이트 변조, DoS 등)
14. 내부 서비스 시스템 가용성 침해 (네트워크 장애유발 악성 코드 등)
15. End-Point 가용성 침해
16. 정보 유출
17. 임직원의 고의적 행위에 의한 정보 유출(고객 개인정보 유출 및 도용, 내부 기술자료 등)
18. 임직원의 실수에 의한 정보 유출(회사 자산의 분실, 메일 전송 오류, 바이러스 감염 등)
19. 외부인의 회사 업무 수행 과정에서 정보 유출
20. 기타 법률과 정보보호 정책 및 지침에서 금지하고 있는 행위

끝.

**부 칙**

**(시행일)** 이 정책은 2018. 10. 05 부터 시행한다.