DOC-POL-003

**생활보안 지침**

개정번호 : 1.00

**㈜1 Shop**

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

**목 차**

[**제1장** **개 요 6**](#_Toc381344509)

[제1조 목적 6](#_Toc381344510)

[제2조 적용대상 6](#_Toc381344511)

[**제2장** **책임과 의무 6**](#_Toc381344512)

[**제1절** **정책 준수 6**](#_Toc381344513)

[제3조 정보보호 의무의 이행 6](#_Toc381344514)

[제4조 자산 보호 6](#_Toc381344515)

[제5조 보안사고 신고 7](#_Toc381344516)

[**제2절** **인력 보안 7**](#_Toc381344517)

[제6조 입사 시 보안 준수 7](#_Toc381344518)

[제7조 고용 중, 업무 변경 및 퇴사 시 보안 준수 8](#_Toc381344519)

[제8조 교육 및 인식 제고 9](#_Toc381344520)

[**제3절** **상벌 9**](#_Toc381344521)

[제9조 포상 9](#_Toc381344522)

[제10조 징계 10](#_Toc381344523)

[**제3장** **생활보안 11**](#_Toc381344524)

[**제1절** **문서 관리 11**](#_Toc381344525)

[제11조 문서 보안 11](#_Toc381344526)

[**제2절** **업무용 단말기 11**](#_Toc381344527)

[제12조 지급 및 반납 11](#_Toc381344528)

[제13조 공용 기기 관리 12](#_Toc381344529)

[제14조 업무용 단말기 보안 설정 12](#_Toc381344530)

[제15조 저장 장치, 주변기기 관리 및 폐기 13](#_Toc381344531)

[**제3절** **계정 및 비밀번호 13**](#_Toc381344532)

[제16조 계정관리 13](#_Toc381344533)

[제17조 비밀번호 관리 14](#_Toc381344534)

[**제4절** **제3자 보안관리 15**](#_Toc381344535)

[제18조 외부인 계약 시 보안 통제 15](#_Toc381344536)

[제19조 외부 위탁 계약 시 보안통제 16](#_Toc381344537)

[제20조 외부인 업무 환경 구성 17](#_Toc381344538)

[제21조 외부인의 보안 통제 17](#_Toc381344539)

[제22조 외부인 계약 종료 시 통제 17](#_Toc381344540)

[**제5절** **안전한 인터넷 사용 18**](#_Toc381344541)

[제23조 네트워크 사용 18](#_Toc381344542)

[제24조 인터넷 사용 18](#_Toc381344543)

[제25조 무선접근 금지 19](#_Toc381344544)

[제26조 전자메일의 사용 19](#_Toc381344545)

[**제6절** **출입 보안 19**](#_Toc381344546)

[제27조 출입 통제 원칙 19](#_Toc381344547)

[제28조 보안구역의 설정 20](#_Toc381344548)

[제29조 사무실 출입 관리 20](#_Toc381344549)

[**제7절** **업무 환경 보안 21**](#_Toc381344550)

[제30조 책상 정리 21](#_Toc381344551)

[제31조 통신 장비의 사용 21](#_Toc381344552)

[제32조 모바일 기기의 사용 22](#_Toc381344553)

[제33조 원격 작업 22](#_Toc381344554)

[**제8절** **소프트웨어 보안 관리 22**](#_Toc381344555)

[제34조 불법 소프트웨어 관리 23](#_Toc381344556)

[제35조 백신 및 OS 업데이트 23](#_Toc381344557)

[**제4장** **개인정보보호 24**](#_Toc381344558)

[**제1절** **개인정보보호 24**](#_Toc381344559)

[제36조 개인정보 처리자의 지정 24](#_Toc381344560)

[제37조 개인정보보호 서약서 24](#_Toc381344561)

[제38조 개인정보보호 교육 25](#_Toc381344562)

[**제2절** **라이프 사이클 별 보호 25**](#_Toc381344563)

[제39조 개인정보의 수집 25](#_Toc381344564)

[제40조 개인정보의 이용 및 저장 27](#_Toc381344565)

[제41조 개인정보의 제공 27](#_Toc381344566)

[제42조 개인정보의 파기 29](#_Toc381344567)

1. **개 요**
2. **목적**

본 지침은 ㈜1 Shop(이하 ‘회사’라고 한다)에 근무하는 사용자에 의해 발생될 수 있는 정보 유출, 변조, 오남용, 삭제 등 각종 사고를 최소화 하기 위해 사무실에서 사무실에서 임직원 및 외부인이 준수해야 할 정보보호 활동과 생활 속에서의 보안을 정하는 것을 목적으로 한다.

1. **적용대상**

본 지침은 회사 내 업무 공간과 모든 임직원 (계약직, 파견직 포함) 및 제3자를 포함하여 적용한다.

1. **책임과 의무**
2. **정책 준수**
3. **정보보호 의무의 이행**
4. 정보보호 정책 및 하위 지침을 숙지 및 준수하여야 하며 담당 업무에 적용하여야 한다.
5. 정보보호 정책 및 하위 지침을 위반하여 회사에 손실을 입히거나 이미지를 훼손한 경우에는 관련 사규에 따라 징계할 수 있다.
6. **자산 보호**
7. 정보자산은 해당 자산을 사용하는 부서에서 자산목록을 관리하여야 하며, 보호 할 의무가 있다.
8. 회사 내에서 사용하는 자산은 반드시 허가되고 보호 등급이 분류된 후 사용되어야 하며, 인가되지 않은 자산 사용이 적발될 시 그 책임을 물을 수 있다.
9. 임직원은 회사에서 제공한 모든 정보 자산을 업무 목적 이외에 개인적인 목적이나 이익을 위하여 사용할 수 없다.
10. 임직원은 인가된 자산에 대해서만 접근이 가능하며, 비인가 자산에 대해서는 불법적인 접근을 시도하지 않아야 한다
11. **보안사고 신고**
12. 임직원은 허가된 범위 내에서 정보자산을 이용할 권한을 가지며, 위법· 위규 사용에 의한 보안사고의 발생에 대한 최종책임은 해당 임직원에게 있다.
13. 임직원은 보안사고 발생 또는 이상 징후 발견 시 부서장 또는 정보보호 최고책임자에게 신고할 의무를 가진다.
14. 회사 중요정보의 공개, 누설, 분실, 유출에 관련한 보안사고 발생 시 해당 정보 관련자는 보안사고의 대응 및 조사에 성실히 협조할 의무가 있다.
15. 보안사고 조사를 위해 정보보호최고책임자의 협조 요청을 받은 부서 및 근무자는 보안사고 대응 및 조사에 성실히 협조할 의무가 있다.
16. **인력 보안**
17. **입사 시 보안 준수**
18. 정보보호 최고책임자는 채용 및 계약 예정자(용역회사를 통해 채용되는 경우 포함)에 대해 신원확인을 실시할 수 있다. 단, 조사 내용이 법규에 의해 제한되는 사항인 경우 반드시 채용 및 계약 예정자에게 서면으로 신원확인에 대한 동의를 받아야 한다.
19. 민감한 직무 담당자에 대해서는 채용 시 혹은 직무 할 당시 강화된 신원확인을 실시할 수 있다.
20. 모든 직원은 채용 시 기밀유지업무를 포함한 “정보보호 서약서” 및 “비밀유지 서약서”에 서명하여야 한다.
21. 정보보호 서약서 및 비밀유지 서약서를 제출하지 않는 자는 채용 및 계약할 수 없다.
22. **고용 중, 업무 변경 및 퇴사 시 보안 준수**
23. 임직원은 연1회 “윤리강령 및 윤리경영 실천지침 준수서약서” 및 “비밀유지 서약서”의 양식에 따라 서약서를 작성하여야 한다.
24. 임직원 중 개인정보를 취급해야 하는 인력은 개인정보 처리업무를 수행하기 전에 “개인정보보호 서약서”의 양식에 따라 서약서를 작성하여야 한다
25. 모든 퇴사 직원은 공개된 정보 혹은 개인적으로 보유한 정보를 제외한 모든 회사 관련 정보를 퇴사 시 직속 관리자 책임 하에 삭제 또는 반납한다.
26. 각종 서버 및 시스템에 접근권한을 가지고 있는 직원이 퇴사하게 될 경우 해당 직원은 모든 정보자산을 반납해야 하며, 시스템 접근 권한도 퇴사일로부터 1일 이내 삭제하거나 비활성 상태로 분류하여 관리한다. 단, 공용 계정을 사용하는 경우는 비밀번호를 변경한다.
27. 직원의 퇴사 시 정보보호 관리자는 다음과 같은 책임을 수행해야 한다.
28. 회사 관련 정보 및 자산의 반납 확인
29. 시스템 관리자에게 퇴사자의 권한 삭제 통보
30. 퇴사자의 업무수행권한 종료
31. 정보보호서약서 징구
32. 정보보호 관리자는 제5항의 각 호의 사항을 확인한 후 인사부서에 그 결과를 통보해야 하며, 인사부서에서는 정보보호 관리자의 확인이 있은 후 퇴직처리 해야 한다.
33. **교육 및 인식 제고**
34. 모든 임직원 및 제3자는 정보보호최고책임자가 정한 시간에 맞추어 해당 교육을 이수하여야 한다. **단, 업무수행을 목적으로 불가피하게 교육을 이수하지 못하는 경우에는 본부장 및 정보보호 최고책임자의 승인이 있다면 예외처리 할 수 있다. (교육을 이수하지 못하는 경우에는 온라인 교육, 교육을 들을 사람이 전파 교육을 하는 등 절차가 있어야 한다.)**
35. 정보보호 담당자는 임직원의 보안교육 효과를 제고할 수 있는 다양한 방법을 고안하여 보안교육 계획에 반영하고 이를 시행하여야 한다.
36. 모든 임직원은 정보보호 담당자가 정한 보안교육 방법(정보보호 및 개인정보보호 업무 지침 제51조)을 반드시 따라야 한다.
37. **상벌**
38. **포상**
39. 정보보호 최고책임자, 개인정보 관리책임자는 다음과 같은 임직원에 대하여 대표이사에게 포상을 건의할 수 있다.
40. 회사의 중요정보 혹은 개인정보가 유출 및 유출 가능성을 인지 후 차단했다고 인정되는 임직원
41. 회사의 정보보호 활동을 외부 기관 및 기업에 인식하게 하여 그로 인한 매출이 발생되도록 노력한 임직원
42. 기타 회사 정보보호 체계의 운영에 있어 그 공이 인정되는 임직원
43. **징계**
44. 정보보호 최고책임자, 개인정보 관리책임자는 다음과 같은 임직원에 대하여 대표이사에게 징계를 건의할 수 있다.
45. 회사의 중요정보 혹은 개인정보를 유출하려고 하거나 실제 정보가 유출된 행위의 주요 행위자인 임직원
46. 회사의 중요정보 혹은 개인정보의 유출사실을 인지하고도 보고 혹은 차단조치를 수행하지 않은 임직원
47. 보안위반 행위가 경미하다 하더라도 반복적으로 위반하거나 재발의 위험이 높은 임직원
48. 기타 회사 정보보호 체계를 운영하지 못하도록 행위 한 것이 인정되는 임직원
49. 임직원과 외부인의 정보보호 위반 사항
50. 침해
51. 중요 보안 구역의 물리적 침입
52. 외부 서비스 시스템 가용성 침해 (사이트 변조, DoS 등)
53. 내부 서비스 시스템 가용성 침해 (네트워크 장애유발 악성 코드 등)
54. End-Point 가용성 침해
55. 정보 유출
56. 임직원의 고의적 행위에 의한 정보 유출(고객 개인정보 유출 및 도용, 내부 기술자료 등)
57. 임직원의 실수에 의한 정보 유출(회사 자산의 분실, 메일 전송 오류, 바이러스 감염 등)
58. 외부인의 회사 업무 수행 과정에서 정보 유출
59. 기타 법률과 정보보호 정책 및 지침에서 금지하고 있는 행위
60. **생활보안**
61. **문서 관리**
62. **문서 보안**
63. 비밀 및 대외비 등급의 문서는 원칙적으로 사외 반출이 불가하며, 업무 수행상 불가피하게 반출할 경우 정보보호 관리자의 승인 후 반출한다.
64. 비밀로 분류된 문서는 출력하여 사용하지 않는 것을 원칙으로 하며, 불가피한 경우 사용 즉시 파기하여야 한다.
65. 모든 출력물은 반드시 회사 내부의 지정된 프린터에서 인쇄하며 인터넷을 이용한 외부 프린트는 금한다.
66. 출력된 모든 문서는 출력자가 즉시 회수하여야 한다.
67. 회사의 중요정보가 포함된 문서는 문서 세절기를 이용하여 폐기한다.
68. 회사의 중요정보가 포함된 문서는 이면지로 활용할 수 없다.
69. 원칙적으로 비밀 문서는 개인 PC에 저장될 수 없으나, 부득이한 경우 암호화하여 저장하고 PC 내 저장된 정보를 해당 업무 목적 달성 직후 반드시 삭제 하여야 한다.
70. **업무용 단말기**
71. **지급 및 반납**
72. PC 담당자는 임직원에게 PC 지급 시 바이러스 백신 등 회사가 지정한 보안소프트웨어를 설치하여 제공하도록 한다.
73. 임직원은 지급 PC에 회사의 정보시스템을 침해하거나 우회할 수 있는 하드웨어를 임의로 설치해서는 안 된다. 업무상 필요성이 인정되는 경우에 부서장의 승인을 득하여 요청한 사용자 PC에 별도 하드웨어를 설치 할 수 있다.
74. 임직원은 지적재산권을 준수하기 위해 다음 각 호를 준수하여야 한다.
75. 비 인가된 추가 복사본 작성을 금지한다.
76. 소프트웨어의 불법 변경을 금지한다.
77. 사용권 증명서를 보관한다.
78. 불법 소프트웨어 사용을 금지한다.
79. **공용 기기 관리**
80. 전화 및 팩스 등 통신장비는 업무와 관련되지 않은 개인적인 용도로 사용할 수 없다.
81. 팩스를 활용하여 정보를 전송할 경우, 잘못된 번호로 전송되지 않게 주의해야 한다.
82. 중요한 정보를 담고 있는 서류를 팩스로 받는 경우에는 도착하는 즉시 회수하여야 한다.
83. 중요한 정보는 전화를 이용하여 음성으로 주고받아서는 안 된다.
84. **업무용 단말기 보안 설정**
85. 모든 개인용 컴퓨터는 바이러스 방어 프로그램을 사용하여야 하며 모든 파일 및 프로그램은 주기적으로 바이러스 확인을 하여야 한다.
86. 바이러스 방어 프로그램은 주기적으로 업데이트 하여야 한다.
87. 바이러스에 감염된 징조가 있는 경우 즉시 네트워크 연결을 해제하고 정보보호 최고책임자에게 이를 보고한 후 조치 받아야 한다.
88. 회사에서 제공하는 것을 제외한 개인 소유의 모든 외장 및 휴대용 저장장치(노트북, 태블릿, USB 등)는 사용을 자제하여야 한다.
89. 모든 컴퓨터는 화면보호기를 작동하여야 하며 작동시간은 10분 이하의 주기로 관리하여야 한다.
90. 개인용 컴퓨터에 비밀번호를 설정하여야 하며 업무 중 자리 이석 시에는 화면을 잠그도록 한다.
91. 노트북 컴퓨터를 외부에서 사용할 때는 도난 등에 대비하여 특별히 관리하여야 한다.
92. **저장 장치, 주변기기 관리 및 폐기**
93. 임직원은 업무용 이외의 USB, 외장하드와 같은 휴대용 저장장치의 사용을 금지한다.
94. 업무상 휴대용 저장장치의 사용이 필요한 경우에는 회사 소유의 휴대용 저장장치를 이용한다.
95. 휴대용 저장장치는 시건장치가 되어 있는 서랍 또는 사물함에 보관하여야 한다.
96. 휴대용 저장장치의 폐기시에는 저장된 내용을 복구할 수 없는 방법(Low Format, 물리적 파기 등)을 이용하여 파기하여야 한다.
97. **계정 및 비밀번호**
98. **계정관리**
99. 사용자 계정은 개인별로 구별되는 계정을 사용하는 것을 원칙으로 한다.
100. 계정 및 비밀번호는 자신 이외의 모든 타인(임직원, 가족, 제3자 등)과 공유하여서는 안 된다.
101. 병가나 휴직 등의 사유로 1개월 이상 계정을 사용하지 않을 경우에는 계정 사용중지를 서버/PC담당자에게 요청하여야 한다.
102. **비밀번호 관리**
103. 원칙적으로 사용자 패스워드에 대한 보안관리 책임은 각 사용자에게 있다.
104. 비밀번호는 비밀로 유지하고 타인에게 노출하지 않도록 한다. 패스워드가 노출된 것으로 의심될 경우 즉시 패스워드를 변경해야 한다.
105. 비밀번호를 별도의 문서에 적어 놓거나 보호되지 않은 형태로 PC에 저장해서는 안 된다.
106. 웹사이트나 메일 클라이언트 등 각종 응용프로그램에서 제공하는 패스워드 자동 저장기능을 사용해서는 안 된다.
107. 임시로 부여 받은 패스워드는 최초 로그인시 반드시 새로운 패스워드로 변경하여야 한다.
108. 업무상 부득이한 사유(서비스 모니터링 등)로 타인에게 계정과 패스워드를 알려주었을 때에는 관련 업무가 끝난 즉시 패스워드를 변경하여야 한다.
109. 패스워드는 다음과 같은 기준에 준하여 설정한다.
110. 문자, 숫자, 특수문자 조합으로 이루어진 최소한 8자리 이상의 것을 사용하고 주기적(반기1회) 으로 변경한다.
111. 주민번호, 전화번호, 생일, 반복적 숫자, 아이디와 동일한 패스워드 등 유추하기 쉬운 것은 사용하지 않는다.
112. 사전에 등록된 단어, 장소명 또는 속어를 사용하지 않는다.
113. 일정한 패턴의 반복을 가지고 있는 문자열의 조합을 사용하지 않는다. (예시: qwer, 1234)
114. **제3자 보안관리**
115. **외부인 계약 시 보안 통제**
116. 개인정보 관리자 및 정보보호 관리자는 계약서 검토 시 해당 용역 업무의 특성을 고려한 보안 요구사항에 대한 SLA 여부 확인 후, 별첨서류에 SLA를 반드시 넣어야 한다.
117. 계약서에 반영되는 보안 요구사항은 다음과 같다.
118. 업무 수행 중 취득한 정보에 대한 누설 금지 조항
119. 계약 완료 시점에서 정보자산의 반환, 폐기 등의 보안 관련 조항
120. 개인정보보호 및 정보보호 관련 법적 조항, 감독기관의 보안규정 및 지침 준수에 대한 책임사항
121. 개인정보보호를 포함한 보안 위반 사항 발생 시 책임 조항 (손해배상 조항)
122. 보안사고, 침해보고, 조사 동의사항
123. 계약 의무사항에 대한 내‧외부 보안 감사에 대한 권한 (감사권 수용)
124. 외주업체의 개인정보 처리 활동에 대한 보고, 모니터링 및 감사 권한 등
125. 기타 일반 보안 관련 사항
126. 계약서에 반영되는 보안위험 및 보안대책은 다음과 같다.
127. 데이터 인수/인계에 관한 사항
128. 전산자원의 보관에 관한 사항
129. 악의적 소프트웨어에 대한 통제 방안
130. 작업시간, 출입장소 등 작업 방법에 관한 사항
131. 비상사태 발생 시의 응급조치에 관한 사항
132. **외부 위탁 계약 시 보안통제**
133. 계약부서의 장은 계약서 상에 다음 각 호와 같은 보안 요구사항을 명시하여야 한다.
134. 회사의 정보보호 규정 준수 의무
135. 정보자산을 보호하기 위한 절차
136. 자료의 손실 또는 변경 등과 같은 조직의 자산에 대한 훼손이 발생했음을 판단할 수 있는 절차
137. 계약의 종료나 인수 시점에서 정보자산의 반환 또는 파손을 확인할 수 있는 방법
138. 정보자산의 복사나 유출에 대한 제약 사항
139. 정보보호 관련 법적 요구사항을 만족시키는 방법 (예 : 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등)
140. 지적 재산권과 저작권 부여 및 공동 작업에 대한 보호방법
141. 접근통제 방안
142. 허용된 접근방식, ID/PW와 같은 신분확인 수단의 사용과 통제
143. 사용자 접근 및 권한에 대한 허가 절차
144. 서비스를 이용할 수 있는 인가자 리스트와 이들과 관련된 권한 유지에 필요한 사항
145. 아웃소싱 업체를 대상으로 하는 모니터링 및 권한 삭제 권리
146. 연 1회 이상 업무 및 정보보호에 대한 회사 및 외부자에 의한 감사 권리
147. 아웃소싱 계약자를 포함하여 아웃소싱에 관련된 모든 자들에게 보안책임을 주지시키기 위한 절차
148. 재난이 발생하였을 경우에 서비스의 가용성을 유지하기 위한 방법
149. 보안관련 계약 위반에 대한 처리에 관한 사항
150. 보안사고 등에 대한 보고, 통지 및 조사
151. **외부인 업무 환경 구성**
152. 외부인이 사내에서 업무를 하는 경우에는 임직원과 분리된 공간에서 작업해야 하며, 물리적인 분리가 힘든 경우에는 정보보호관리자의 승인 후 임직원과 같은 공간에서 작업이 가능하다.
153. 외부인은 임직원이 사용하는 네트워크를 사용하지 못 하며, 별도로 구성된 외부망을 이용해야 한다.
154. **외부인의 보안 통제**
155. 정보보호 최고책임자는 아웃소싱 업체에 대하여 보안점검을 실시할 수 있다.
156. 계약부서는 정보보호 최고책임자의 보안점검에 적극 협조하여야 한다.
157. 계약부서는 아웃소싱 업체에 대한 보안점검이 필요하다고 판단되는 경우 명확한 사유를 표명하여 정보보호 최고책임자에게 보안점검을 요청할 수 있다.
158. **외부인 계약 종료 시 통제**
159. 보유 중인 모든 정보자산을 반환해야 하며 개인 PC, 노트북, 저장장치 등에 포함된 지적 자산과 관련된 모든 정보는 삭제한다.
160. 물리적‧논리적 권한을 반납하고 삭제하며 정보보호 관리자에게 이에 대한 확인을 받아야 한다.
161. 업무 완료 시 특별한 허가를 받지 않는 한 취득한 어떤 정보자산도 외부용역업체의 소속회사나 외부인력 개인이 보유해서는 안 된다.
162. 임직원과 동일하게 비밀 유지 서약서 및 정보보호 확인서를 징구 해야한다.
163. **안전한 인터넷 사용**
164. **네트워크 사용**
165. 임직원 별로 부여된 네트워크 IP 주소를 임의로 변경하지 않는다.
166. 네트워크 선을 임의로 개설하거나 인터넷 통신이 가능한 프로그램을 가동하여 PC 또는 서버를 인터넷에 연결해서는 안 된다.
167. 외부에서 인터넷으로 회사 내부의 시스템에 접속하는 것을 금지한다.
168. **인터넷 사용**
169. 업무와 관련되지 않은 인터넷 사이트 접속을 하여서는 안 되며, 다음의 사이트 접속은 금지한다.
170. 음란 사이트: 음란사진, 동영상 등을 제공하는 사이트(뉴스그룹 포함)
171. 무단 복제 사이트: 무단 복제된 프로그램이나 파일을 제공하는 사이트
172. 해킹 사이트: 해킹과 관련된 정보를 담고 있는 사이트
173. 기타 접속 금지의 필요성이 인정되는 사이트(만화/게임, 인터넷방송, 증권, 도박 등)
174. 신뢰할 수 있는 웹 사이트를 방문한 경우를 제외하고는 자바와 Active-X 기능의 사용에 주의하여야 한다.
175. 근무시간 중 회사 네트워크 성능 저하를 초래할 수 있는 업무와 무관한 인터넷 사용을 하여서는 안 된다.
176. 개인정보와 회사의 중요 정보는 암호화하지 않고 인터넷 홈페이지 등에 게시하거나 전송하여서는 안 된다.
177. **무선접근 금지**
178. 사내에서 사용하는 무선AP는 별도의 네트워크로 구성하여 운영한다.
179. 임직원의 데스크탑 및 노트북의 무선 AP 접속을 제한한다.
180. 스마트폰 및 태블릿PC 등의 테더링 기능을 활용하여 인터넷 연결을 하여 사용하지 않는다.
181. **전자메일의 사용**
182. 회사와 관련된 모든 정보는 그룹웨어를 통해서만 전송해야 하며, 인터넷 메일(Web Mail 등) 및 메신저 등을 통해 전송할 수 없다.
183. 전자메일은 업무적인 목적을 위해서만 사용되어야 하고 불법적인 용도(스팸메일, 바이러스 유포 등)나 불순한 목적으로 사용되어서는 안 된다.
184. 발신인이 확실하지 않거나 바이러스가 의심되는 메일은 읽지 않고 즉시 삭제한다.
185. **출입 보안**
186. **출입 통제 원칙**
187. 정보보호 최고책임자는 제한구역의 출입통제를 위하여 카드 잠금장치, 지문인식 잠금장치 등 출입통제 장치를 설치 및 운영하여야 한다.
188. 제한구역을 출입하는 모든 출입자는 반드시 출입증을 패용하여야 한다.
189. 외부인력의 제한구역 출입은 업무상 필요에 따라 결정되어야 하며, 수행직원은 외부인력과 동행하여 제한구역에서의 활동을 지속적으로 감독하여야 한다.
190. 통제구역의 출입문에는 출입자가 통제구역임을 쉽게 인지할 수 있도록 별도의 표시를 하여야 한다.
191. 통제구역은 출입통제를 위하여 별도의 출입통제장치를 설치하여야 한다.
192. 통제구역의 출입문은 자동으로 잠김이 가능하여야 한다.
193. 물리보안담당자는 통제구역 출입자의 출입로그를 3개월 이상 보관하여야 한다.
194. 모든 임직원은 비인가자의 불법접근 또는 시도를 인지한 경우, 정보보호최고책임자 및 정보보호 관리자에게 즉시 보고하여야 한다.
195. 정보보호 관리자는 통제구역의 출입로그를 분기 1회 점검 하여야 한다.
196. **보안구역의 설정**
197. 정보보호 최고책임자는 회사의 주요 정보자산 및 관련 시설에 대한 보안강화를 위하여 다음 각 호와 같은 보호구역을 지정 및 운영하여야 한다.
198. 제한구역: 회사의 중요정보가 사용되어 임직원은 출입 가능하나, 외래인 및 방문자에 대한 출입 안내가 요구되는 구역
199. 통제구역: 회사의 핵심적인 정보가 사용 및 보관되어 임직원 또한 출입 허가를 득한 자만 출입이 가능한 구역
200. 지정된 보안구역은 “보안구역 현황”에 따른다.
201. **사무실 출입 관리**
202. 임직원은 출입증을 쉽게 인지할 수 있도록 외부에 노출하여 패용하여야 한다.
203. 임직원은 사내에 출입증을 패용하지 않은 자가 출입하지 못하도록 하여야 하며, 출입증을 패용하지 않은 인원을 발견하면 즉시 출입구로 안내해야 한다.
204. 임직원은 출입 시 외부 인원이 따라 들어오지 못하도록 유의해야 한다.
205. 외부인과 사무실에서 접견해야 할 경우에는 회사 주요 정보가 노출 혹은 유출되지 않도록 담당자가 동행하여야 한다.
206. **업무 환경 보안**
207. **책상 정리**
208. 임직원은 업무와 관련된 자료를 개인 책상에 보관할 수 없으며, 반드시 시건장치가 된 서랍 또는 사물함에 보관하여야 한다.
209. 퇴근 시나 이석 시 모든 서랍 및 사물함의 잠금장치를 잠그도록 한다.
210. 노트북, USB, PDA 와 같이 물리적인 이동이나 이탈이 쉬운 기기일 경우, 퇴근 시 시건 장치가 부착된 서랍 등 안전한 장소에 보관하도록 한다.
211. 화면을 통한 정보유출을 방지하기 위하여 화면보호기(10분)가 작동하도록 설정하며, 다시 시작할 때 로그인 화면표시가 되도록 적용하여야 한다.
212. 자리를 비울 때에는 <컴퓨터 잠금: Window key + L>기능을 사용하여 제3자에 의한 접근을 막아야 한다.
213. 자리를 비울 때는 비밀문서나 문서 출력물을 책상 위에 방치하지 않는다.
214. 퇴근 시에는 PC의 전원을 반드시 차단해야 한다.
215. **통신 장비의 사용**
216. 전화 및 팩스 등 통신장비는 업무와 관련되지 않은 개인적인 용도로 사용할 수 없다.
217. 팩스를 활용하여 정보를 전송할 경우, 잘못된 번호로 전송되지 않게 주의해야 한다.
218. 중요한 정보를 담고 있는 서류를 팩스로 받는 경우에는 도착하는 즉시 회수하여야 한다.
219. 중요한 정보는 전화를 이용하여 음성으로 주고받아서는 안 된다.
220. **모바일 기기의 사용**
221. 스마트폰 및 태블릿PC는 사내 무선AP에 물리적주소(MAC)을 등록하여 이용한다.
222. 스마트폰 및 태블릿PC 등을 활용하여 업무자료 등 중요정보의 저장 및 전송을 금지한다.
223. **원격 작업**
224. 임직원은 외부에서 사내의 PC 또는 서버로의 원격 접속을 금지한다.
225. 업무 필요상 접속이 필요한 경우에는 정보보호 관리자의 승인을 얻은 후 안전한 방법(예시: VPN 등)을 이용하여 접속하여야 한다.
226. 원격 작업자는 PC방과 같이 불특정 다수가 공동으로 사용하는 PC를 통하여 회사의 시스템에 접속하는 것을 금지한다.
227. 원격 작업을 위한 물리적 환경은 불특정 다수로부터 원격 작업자 PC에 대한 물리적 접근 통제나 모니터링이 가능한 장소이어야 한다.
228. 원격작업의 기간이 완료되는 경우 접근권한, 장비 등을 회수하여야 한다.
229. **소프트웨어 보안 관리**
230. **불법 소프트웨어 관리**
231. 모든 PC에는 라이선스(license)가 있는 소프트웨어만을 설치해야 하며, 라이선스는 정보보호 관리자가 보관하여야 한다.
232. 제1항에서 보관되는 라이선스 이외의 소프트웨어를 사용하는 경우 불법소프트웨어 사용으로 간주하며, 그 예는 다음 각 호와 같다
233. 불법 복제한 S/W의 사용, 또는 보조기억장치(Disk, CD, 디스켓 등)에 담아 보유할 경우
234. 정품 소프트웨어 보유수량에 대한 수량을 초과하여 설치한 경우
235. Shareware 또는 Trial, Evaluation 등의 S/W를 Crack 등(시리얼번호 도용, 날짜 Patch 등)을 이용하여 원본 파일을 조작해 사용할 경우
236. 기타 소프트웨어 사용권 계약을 위반할 경우
237. 필요한 소프트웨어는 정보보호 관리자에게 구매 및 사용신청을 통하여 사용해야 한다.
238. 업무 목적상 공개용(Freeware)이나 Shareware(날짜제한이 포함된 S/W포함)등을 사용하여야 할 경우에는 정보보호 관리자의 사전 승인 및 사용권 계약을 확인하여 불법조항에 해당하지 않도록 확인한 후 사용해야 한다.
239. 회사에서 보안상 사용을 권장하는 소프트웨어를 기본적으로 설치해야 한다.
240. **백신 및 OS 업데이트**
241. 모든 업무용 PC 및 노트북 PC에는 반드시 회사에서 제공하는 바이러스 백신 프로그램을 설치하여야 한다.
242. **PC사용자는 바이러스 백신 프로그램의 월 1회 예약 업데이트 기능을 이용하여 최신 버전으로 유지하여야 한다. (주기가 너무 길다. 자동 업데이트 또는 일 1회 이상 업데이트)**
243. 모든 사용자는 주기적으로 혹은 바이러스 감염이 의심되는 경우 바이러스 감염 여부를 검사하여야 한다.
244. 바이러스 백신의 실시간 감시 기능을 항상 활성화 하여야 한다.
245. PC에 설치된 바이러스 백신 프로그램을 임의로 제거해서는 안 된다.
246. **개인정보보호**
247. **개인정보보호**
248. **개인정보 처리자의 지정**
249. 개인정보 처리자의 범위는 회사 내에서 고객들의 개인정보 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원도 포함될 수 있다.
250. 개인정보 처리자는 고객의 개인정보보호와 관련하여 다음 각 호와 같은 역할 및 책임을 이행하여야 한다.
251. 개인정보보호 활동 참여
252. 내부관리계획의 준수 및 이행
253. 개인정보의 기술적․관리적 보호조치 기준 이행
254. 직원 또는 제3자에 의한 위법․부당한 개인정보 침해행위에 대한 점검 등
255. 기타 고객의 개인정보보호를 위해 필요한 사항의 이행
256. **개인정보보호 서약서**
257. 개인정보를 취급해야 하는 임직원은 개인정보 처리업무를 수행하기 전에 “개인정보보호 서약서” 의 양식에 따라 서약서를 작성하여야 한다.
258. 개인정보보호 서약서를 작성하지 않는 경우 개인정보 처리 업무를 할 수 없다.
259. **개인정보보호 교육**
260. 개인정보 관리자는 개인정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오․남용 또는 유출 등을 적극 예방하기 위해 임직원을 대상으로 매년 정기적으로 연 1회 개인정보보호 교육을 실시한다.
261. 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.
262. 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 관리책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.
263. **라이프 사이클 별 보호**
264. **개인정보의 수집**
265. 개인정보는 정보주체에게 사전에 동의를 받은 경우에 수집할 수 있으며 그 수집 목적의 범위에서만 이용할 수 있다.
266. 회사는 다음 각 호의 사항을 정보주체에게 알린 후 개인정보를 수집하여야 한다.
267. 개인정보의 수집 및 이용 목적
268. 수집하려는 개인정보의 항목
269. 개인정보의 보유 및 이용 기간
270. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익에 대한 사항
271. 제2항의 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
272. 회사는 인터넷 홈페이지를 통한 회원가입, 오프라인 교육 수강생 모집, 고객사 담당자 연락처 등 고객이 기재하고 연락처를 제공하기로 명확한 의사를 표명하거나 사회통념상 동의의사가 있었다고 인정되는 정보를 수집한다.
273. 계약 등의 상대방인 정보주체가 만 14세 미만 아동의 법정대리인 등 대리인을 통하여 법률행위 또는 의사표시를 하는 경우에는 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집 및 이용할 수 있다.
274. 회사는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 한다
275. 필요한 최소한의 개인정보를 수집 하여야 하며, 정보주체가 추가 수집에 대해 거부할 수 있는 절차나 시스템이 구성되어 있어야 한다
276. 개인정보 수집 시 아이핀 등 주민등록번호를 대체하는 수단을 제공 하여야 한다.
277. 회사는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하지 않는다. 다만 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다.
278. 수집된 정보를 제공받는 경우, 수집 시 동의획득의 책임이 수집 기관에게 있음을 명시하여야 한다. 또한 위탁관계의 경우 개인정보보호 규정을 위반하지 않도록 감독하여야 한다.
279. 개인정보 수집 시 이용자가 쉽고 명확하게 이해할 수 있는 방법으로 이용자의 동의를 받아야 한다.
280. 동의를 얻어야 할 내용을 이용자가 명확히 인지하고 확인할 수 있도록 표시하여야 한다.
281. 만14세 미만 아동의 동의를 얻을 경우 아동이 쉽게 이해할 수 있는 평이한 표현으로 고지하여야 한다.
282. 이용자로부터 득한 개인정보 수집동의 기록을 보관하여야 한다.
283. **개인정보의 이용 및 저장**
284. 개인정보를 수집 목적 이외의 용도로 제3자에게 제공하려는 경우에는 정보주체로부터 별도의 동의를 받아야 한다. 단, 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우는 제공할 수 있다.
285. 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 제공과 동시에 다음 각 호의 사항에 대한 구체적인 조치를 마련하도록 문서(전자문서를 포함하는 계약서 혹은 확약서 등의 문서)로 요청하여야 한다.
286. 제공받은 개인정보의 이용 목적, 이용 방법, 이용 기간, 이용 형태의 제한
287. 기타 개인정보의 안전성 확보를 위하여 필요하다고 판단되는 사항
288. 이 경우 요청을 받은 자가 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 회사에 문서로 알리도록 하여야 한다.
289. 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공하는 회사와 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확히 하여야 한다.
290. 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명 혹은 법인명과 연락처를 함께 알려야 한다.
291. 통계작성 및 학술연구 등의 목적으로 개인정보 제공이 필요한 경우에는 특정 개인을 알아볼 수 없는 형태로 개인정보를 가공한 경우에만 가능하며 그 외의 사항에 대하여는 개인정보보호 관리자 및 정보보호최고책임자의 승인이 있어야 제공이 가능하다.
292. **개인정보의 제공**
293. 개인정보를 제3자에게 제공하기 위해서는 정보주체로부터 서면, 공인인증서 전자서명이 있는 전자문서, 고객 비밀번호 인증 또는 휴대전화 인증 등의 유무선 통신방식으로 동의를 받아야 한다.
294. 개인정보의 제공에 대한 정보주체의 동의를 받은 경우 회사는 사전에 다음 각 호의 사항을 정보주체에게 알려야 한다.
295. 개인정보를 제공받는 자 (성명 혹은 법인명, 연락처)
296. 개인정보를 제공받는 자의 개인정보 이용 목적
297. 제공하는 개인정보의 항목
298. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
299. 동의를 거부할 권리가 있다는 사실과 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용
300. 개인정보 처리 위탁 시 위탁자 정보변경, 개인정보취급위탁 업무의 내용을 변경할 경우 이용자에게 별도 동의절차를 거쳐야 한다.
301. 다음 경우일 경우에만 제3자에게 동의를 받지 않고 개인정보를 제공할 수 있다.
302. 서비스의 제공에 따른 요금정산을 위하여 필요한 경우
303. 법률에 특별한 규정이 있는 경우
304. 개인정보의 제3자 제공과 관련하여 사전에 이용자에게 고지한 사항 중 변경이 발생한 경우 이용자에게 알리고 동의를 받아야 한다.
305. 법규정 혹은 이용자의 동의에 따라 개인정보를 제공할 경우 사안 별 적법성을 확인하고 승인 및 기록을 남기는 등의 절차를 마련하여야 한다.
306. 제3자의 개인정보에 대한 접근권한 부여 시 알 필요 및 할 필요에 기초하여 최소화하고, 접근시도를 기록, 검토하여 개인정보침해를 예방 및 적발할 수 있는 조치가 마련되어야 한다.
307. 이용자 본인 또는 법정 대리인이 요청할 경우 이용자의 개인정보에 대한 제3자 제공 내역을 제공할 수 있어야 한다.
308. 공식계약 시 신청사업자와 제3자간의 계약종료 또는 제공 기관과 이용자와의 계약 종료 또는 이용자 요청 시 이용자의 개인정보 이용 중지 및 삭제 등 제3자가 준수해야 할 정책 및 보안요건의 준수 의무와 위반 시 손해배상 등의 조항이 포함되어야만 추후 문제 발생 시 책임 소재 규명 및 명확한 처리가 가능하다.
309. 제3자의 요구사항 준수여부를 정기보고, 감독 등을 통하여 지속적으로 점검하고 필요시 감사 등 적절한 조치를 수행하여야 한다. 단, 계약관계 상의 사유로 위 활동에 어려움이 있는 경우 계약서 상에 관련 조항을 명시하여야 한다.
310. **개인정보의 파기**
311. 개인정보는 이용 목적의 완료 즉시 파기하여야 한다.
312. 법규 또는 회사에서 별도로 보존연한을 정하는 개인정보는 보존연한 만료 시 폐기하여야 한다. 단, 보존연한 만료에도 불구하고 특별한 사유로 보존기간을 연장해야 하는 경우 개인정보 관리책임자의 승인을 받아야 한다.
313. 개인정보의 파기는 “DOC-POL-002\_정보보호 및 개인정보보호 업무지침”에 정한 바에 따른다.
314. 위탁업체 또는 제3자에게 제공한 개인정보도 함께 지체 없이 파기하여야 한다. 단, 제3자의 파기이행여부를 직접 확인하기 어려운 경우 계약서 상에 파기 관련 조항을 명시하여야 한다.
315. 파기일자 후 파기책임자가 실제로 파기하였는지를 확인하여야 한다.

끝.

**부 칙**

**(시행일)** 이 정책은 2018. 10. 05 부터 시행한다.