기업 채용 정보시스템 프로젝트를 통한 개인정보 암호화 보안

※ 본 프로젝트는 “개인정보 보호법”에 따라 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적 보호조치 중 “암호화”에 대한 프로젝트로 진행하였습니다.

채용 정보시스템의 선정 사유

1. 기업에서 가장 민감한 개인정보가 취급되는 업무로
2. 대부분의 기업에서 내부 감사의 주요 항목이 되어 있는
3. 가장 보안에 민감한 개발 분야이다.
4. 일반 **SI** 프로젝트 수행 과정의 이해 및 그 과정에서의 보안 적용 실무 습득

개인정보 암호화 관련 조치 규정

1. 목적
개인정보 보호법에서는 개인정보에 대한 안전성 확보조치 의무를 규정하고 있으며 그중 하나로 암호화 조치를 수행토록 하고 있다.
개인정보처리자가 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 저장하는 경우 암호화 기준을 제시하고 적용방법 및 적용사례 등을 구현함을 목적으로 한다.

☞ 「개인정보 보호법」 제**24**조(고유식별정보의 처리제한) 제**3**항 및 동법 시행령 제**21**조(고유식별정보의 안전성 확보조치)
☞ 「개인정보 보호법」 제**29**조(안전조치의무) 및 동법 시행령 제**30**조(개인정보의 안전성 확보조치)
☞ 「개인정보 보호법」 시행령 제**30**조(개인정보의 안전성 확보조치) 제**3**항에 따른 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제**2011**-제**43**호) 제**7**조

2. 적용 대상
개인정보 보호법에 따라 고유식별정보(주민등록번호, 여 권 번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 저장하는 개인정보처리자를 대상으로 한다.

3. 암호화 종류 및 특징
ARIA는 대칭키 방식의 국가 암호화 알고리즘으로 **128** 비트 블록 단위로 데이터의 암호화, 복호화를 수행하는 블록 암호 알고리즘이다.
128/192/256 비트 키를 지원하며 **2004**년에 한국산업규격 **KS** 표준으로 제정되었다.
일방향 암호화 방식은 해쉬함수를 이용하여 암호화된 값을 생성하며 복호화 되지 않는 방식이다.
해쉬함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해쉬값 또는 해쉬 코드라 불리는 값을 생성하며, 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해쉬값만으로 입력 메시지를 유추 할 수 없어 전자서명 체계와 함께 데이터의 무결성을 위해 사용된다.
비밀번호와 같이 복호화가 필요 없지만 입력 값의 정확성 검증이 필요한 경우에 사용하고 있다.
대표적인 해쉬함수로는 **SHA-2(SHA-224/256/384/512)**, **RIPEMD-160** 등과 국내에서 개발한 **HAS-160**이 있다.

4. 암호화 관련 주요내용
정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제**15**조 제**6**항에 따른 ‘개인정보의 기술적·관리적 보호조치 기준 제**6**조’ (방송통신위원회 고시 제**2012-50**호)
제**6**조(개인정보의 암호화)
①정보통신서비스 제공자등은 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.
②정보통신서비스 제공자등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.

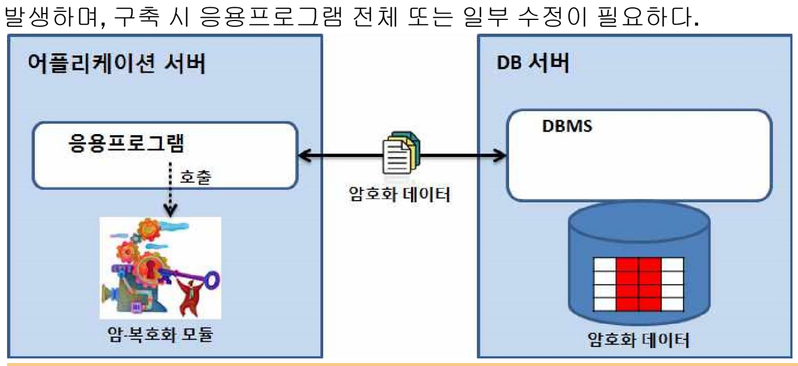
※ 안전한 암호 알고리즘이 무엇인가요?
안전한 암호 알고리즘은 국내외 전문기관(**KISA, NIST, ECRYPT, CRYPTREC** 등)에서 권고하고 있는 알고리즘을 의미합니다. 본 안내서의 ‘**[표 1]** 안전한 암호 알고리즘(예시)’를 참고하시기 바랍니다.
※ 공공기관은 **IT**보안인증사무국(**http://service1.nis.go.kr**)의 검증필 암호 모듈 또는 제품 참조
※ 암호기술 구현 안내서(**2011.11**, 한국인터넷진흥원). 암호 알고리즘 및 키 길이 이용 안내서(**2009.3**, . 한국인터넷진흥원)

※ 안전한 알고리즘이 다양한 키 길이를 제공하고 있는데, 키 길이에 상관없 이 아무거나 사용해도 되나요?
암호 알고리즘은 키 길이 등에 따른 안전성 유지기간을 가지고 있으므로, 키 길이가 **128** 비트 미만인 대칭키 암호화 알고리즘과 해쉬값 길이가 **112** 비트 이하의 일방향 암호 알고리즘은 사용하지 않도록 권고합니다.

③정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.
1.웹서버에 **SSL(Secure Socket Layer)** 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2.웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
④정보통신서비스 제공자등은 이용자의 개인정보를 개인용컴퓨터(**PC**)에 저장할 때에는 이를 암호화해야 한다.

5. 저장시 암호화
개인정보를 처리하고 관리하는 개인정보처리시스템은 **DB**에 저장된 개인 정보를 암호화하여 저장함으로써 개인정보의 변경, 파괴 및 유출을 방지 해야 한다.

6. 응용 프로그램 자체 암호화 방식
응용프로그램 자체 암호화 방식은 암·복호화 모듈이 **API** 라이브러리 형태로 각 어플리케이션 서버에 설치되고 응용프로그램에서 암·복호화 모듈을 호출하는 방식이다.
DB 서버에는 영향을 주지 않지만 어플리케이션 서버에 암·복호화를 위한 추가 적인 부하가 발생하며, 구축 시 응용프로그램 전체 또는 일부 수정이 필요하다.

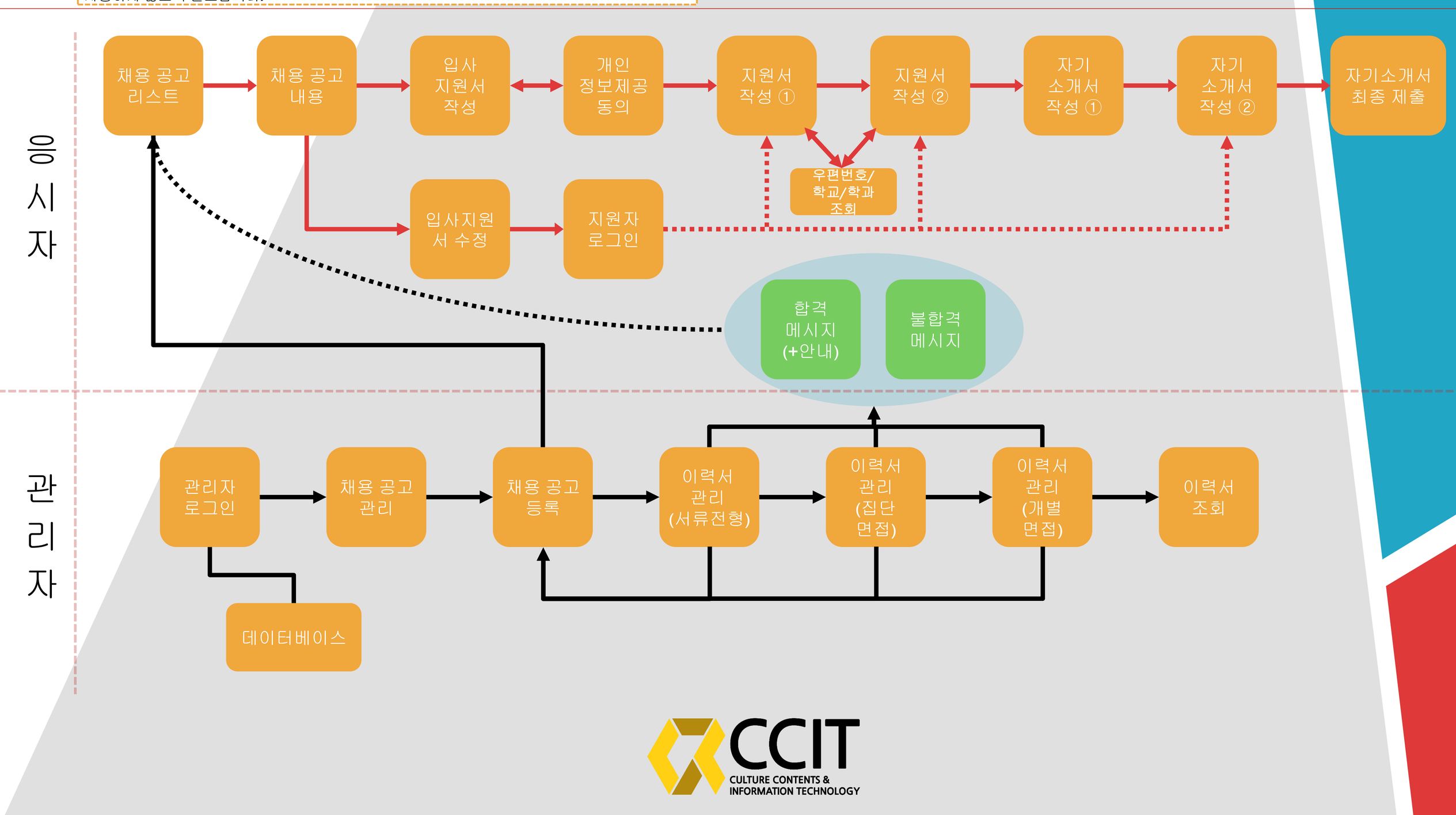


개인정보 암호화 관련 조치 사항

1. 개인정보의 암호화
채용 시스템의 암호화 정보는 이메일(아이디), 패스워드, 전화번호, 핸드폰번호를 암호화하고 있습니다.
패스워드는 일방향 암호화하였고, 이메일, 전화번호, 핸드폰번호를 양방향 암호화하고 있습니다.
패스워드는 암호화하면 복호화되지 않도록 하였으며, **KISA**에서 제공하는 **SHA-256** 알고리즘을 사용하여 암호화하여 저장하고 있습니다.
이메일, 전화번호, 핸드폰번호는 암호화와 복호화가 가능하도록 하였으며, **KISA**에서 제공하는 **ARIA** 알고리즘을 사용하여 암호화하여 저장하고 있습니다. 또한 로그인을 하거나 입사지원서를 작성하여 저장을 할 경우, 저장되는 데이터를 임의의 키로 변환하여 서버로 전송하고 있습니다.
암호화 대상은 정보통신망법, 개인정보보호법에서 암호화를 요구하는 개인정보의 항목은 비밀번호, 바이오정보, 주민등록번호, 신용카드정보, 계좌번호, 여권번호, 운전면허번호, 외국인등록번호이며, 그 외 개인정보에 대해서는 개인정보영향평가 등을 통해 업체 자율적으로 정한 범위에서 암호화하도록 되어 있습니다.

※ 회사에 고객들의 이름, 주소, 전화번호, e-mail, 비밀번호를 저장하고 있습니다. 암호화 대상이 무엇인가 요?
개인정보의 안전성 확보조치 기준 고시 제**7**조에서 암호화 대상은 고유식별정보 (주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보 입니다. 따라서 이 경우에는 비밀번호만 일방향 암호화해서 저장하시면 됩니다.

2. 접속 기록의 보관 및 점검
채용 시스템의 서버의 자체적으로 접근자의 **IP**, 접근시간, 접근한 **URL**주소를 남기도록되어있습니다.
추가적으로 시스템에서 사용자의 접근시간과 접근자의 **IP**, 접근자의 채용관련 정보(채용번호, 접수번호), 접근한 화면 주소, 접근한 화면에 전달된 정보, 현재 화면에 접근하기 이전 화면 주소를 기록하는 기능을 추가하여 로그를 작성하도록 하고 서버의 로그, 사용자 정보와 비교하여 사용자의 접근 기록을 분석할 수 있도록 하였습니다.
3. 개인정보 파기
채용 시스템은 채용이 끝난 후 입사지원서를 작성한 모든 사용자의 정보를 삭제하도록 되어있습니다.
채용진행이 마감이 되면 자동으로 해당 채용의 지원자들의 모든 정보를 삭제합니다.



CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY