PC-02 (상)	1. 계정관리 > 1.2 패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정
취약점 개요	
점검내용	■ 패스워드 설정 정책이 복잡성을 만족하는지 점검
점검목적	■ 안전한 패스워드(*패스워드 설정 기준 참조)를 사용함으로써 무작위 대입공격, 사전공격 등 패스워드 탈취 목적의 공격에 대한 대비를 목적으로 함
보안위협	■ 무작위 대입 공격, 패스워드 추측 공격 등 패스워드가 비교적 단순하거나 비교적 자주 쓰이는 패스워드(예:1q2w3e4r! 등)로 비인가 접근을 시도하는 공격들이 존재함
참고	※ 무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도 ※ 사전 공격(Dictionary attack): 사전에 있는 단어를 입력하여 암호를 알아내거나 해독하는 컴퓨터 공격법 < 패스워드 설정 기준 > 1. 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정 ※ 다음 각 항목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 가. 영문 대문자(26개) 나. 영문 소문자(26개) 다. 숫자(10개) 라. 특수문자(32개) 2. 패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계 (1) Null(공백) 패스워드 사용 금지 (2) 문자 또는 숫자만으로 구성 금지 (3) 사용자 ID와 동일하거나 유사하지 않은 패스워드 금지 (4) 연속적인 문자나 숫자 사용 (예) 1111, 1234, abcd) 사용 금지 (5) 주기성 패스워드 재사용 금지 (6) 전화번호, 생일과 같이 추측하기 쉬운 개인정보를 패스워드로 사용 금지

	3. SAM파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호 사용 권장 (8자로 이루어진 암호 사용 권장) 4. 아래와 같은 암호 설정 지양 Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자명, 대표 업무명 "root", "rootroot", "root123", "123root", "admin", "admin123", "123admin", "osadmin", "adminos"
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windos 8.1, Windows 10
판단기준	**취약** : 암호를 사용하지 않거나, 추측하기 쉬운 문자조합으로 이루어진 짧은 자릿수의 패스워드를 사용하는 경우
조치방법	최소 암호 길이를 해당 기관의 보안 정책에 적합하게 설정
조치 시 영향	일반적인 경우 영향 없음