KISTI 슈퍼컴퓨팅 동향분석 보고서

슈퍼컴퓨팅 보안 기술동향:
NCSA Security Policies and Procedures

그림

슈퍼컴퓨팅본부 융합자원실 슈퍼컴퓨터인프라팀

한국과학기술정보연구원

차 례

1. 서론

본 문서는 NCSA 보안 정책 및 절차를 규정한다. 이는 보안 정책 개발 및 실행, 책임 관리 할당, 그리고 보안 실행 및 점검, 나아가 보안 관련 문제 또는 사고의 해결을 위한 방법을 제공한다.

NCSA의 컴퓨팅 및 지적 환경은 학계, 정부, 그리고 사적 영역에 걸친 연구들을 포함한다. 정보의 민감성 및 교환의 개방성은 이들 각각의 환경에 따라 다르다. 그러나 NCSA의 역사는 이들 각각의 분야에서 이루어진 교류와 협력에 따른 지적 교류 및 교환의 가치를 보여준다. NCSA의 보안 정책 및 기술적 보안의 구조는 연구자들의 자신들의 연구를 수행 할 수 있는 적정 수준의 메커니즘을 제공하기 위하여 설계된다.

NCSA의 보안 전략은 보안 관련 담당자들에 대한 보안 정책 및 절차에 대한 도구 및 교육을 제공하는 것이며 이러한 지식 및 도구를 이용하여 자신들의 보안 업무를 수행하며 이를 점검할 수 있게 한다. 나아가, 중앙화된 보안 점검 및 제어가 기본적인 보안의 보장을 위하여 적용되며 이는 보안의 관리를 제공한다.

NCSA는 국가 또는 국제적 차원의 연구 기관, 정부, 그리고 사적 영역 사용자를 위한 다양한 형태의 컴퓨팅 시스템, 서비스, 그리고 연구 프로젝트를 지원한다. 이는 NCSA의 툴을 사용하는 개별 사용자, 보안 담당자, 또는 기관 등에 대하여 책임을 가지며 이를 통하여 이들의 자산이나 상해, 절도, 그리고 불법적 사용으로부터 사용자들을 보호한다.

NCSA의 기본적인 보안 사항은 아래의 내용을 포괄한다.

- 개인적 자산의 보호 사이트를 포함하여 모든 NCSA 사이트에서 일하는 담당자의 개인 보안
- 화재, 도난, 그리고 불법적 사용을 포함하여 건물, 장비, 그리고 기록물의 물리적 보안
- 민감한 자료의 보안 (세부 항목 규정을 참고). 이는 비공개 및 다른 보안 관련 계약에 대한 수락 내용을 포함한다. 통상적인 공급자들 또는 연구 파트너들은 다른 사람들에게 공개되기를 꺼리거나 계약 내용에 벗어나는 사용을 원치 않는 정보를 제공한다.
- 불법적 사용 또는 서비스 거부를 방지하기 위한 컴퓨팅 시스템이나 네트워크의 관리를 포함하여 고급 컴퓨팅 및 정보 인프라의 보안, 그리고 이들 시스템이 저장하고 있거나 가지고 있는 지적 재산 (문서, 소프트웨어, 그리고 데이터)에 대한 보안

1.1. 사훈

NCSA 보안 정책 및 관련 보안 표준, 가이드라인 또는 절차에 대한 문서는 다양한 NCSA 자산의 신뢰성 있는 보호를 제공하기 위하여 개발되고 있다. 이러한 자산은 자원 (컴퓨터 시스템, 프린터 및 복사기), 정보 (지적 자산), 인프라 (네트워크 및 관련 장비), 또는 연관성 (사적 영역 파트너들과의 계약) 등을 포괄한다. 이러한 자산에 대한 제한을 두지 않고 고려될 수 있는 위협 요소로는 외부로부터의 직접적인 사이버 공격, 내부 직원 또는 사용자에 의한 부적절한 자원의 사용, 민감한 데이터의 우발적 노출, 그리고 자연 재해를 꼽을 수 있다.

NCSA 보안 팀의 역할은 첫째, 민감한 정보의 취급 요령에 대한 사용자 교육 및 이들의 컴퓨터를 보안 유지 상태로 연결하는 방법에 대한 교육. 그리고 둘째, 담당 직원 및 연구원에 대하여 자산의 기밀성, 통합성, 그리고 가용성의 보장을 통한 중앙 임무의 지원에 있다. 다른 NCSA 그룹과의 협력에 있어서 보안 팀은 우리의 네트워크 및 컴퓨팅 시스템에 가해지는 위험에 대한 평가, 감지, 그리고 해결을 통한 우리의 자원을 보호 할 수 있도록 도움을 준다. 이러한 정책 기조는 보안 정책의 기본이 되며 이와 함께 관련 표준 및 절차들은 언급한 목적을 달성하기 위한 모든 NCSA 직원들에 적용된다. 나아가 이는 정책 기조의 유지를 위한 보안 팀의 책임이기도 하며 이를 통하여 지속적인 업데이트 및 사용자 지원을 유지하게 된다.

이러한 정책 및 관련 문서 및 기록들은 모든 NCSA 직원들에게 배포되며 여기에서 직원은 정규직 및 비정규직, 그리고 학생 직원을 포함한다. 이 정책 자료 자체는 민감한 수준이 아니며 비록 공개된다 할 지라도 NCSA 자산을 위협하는 수준이 아니다.

1.2. 정책 범위

NCSA 감독 사무국 (DO: Director's Office)은 보안 구축 및 실행에 대한 모든 책임을 가진다. 사무국의 모든 직원 또는 모든 NCSA 지국장 (DD : Division Director)들은 자신들의 지역에 있어서 보안 정책 및 절차에 대한 자문을 수행할 수 있다. 각각의 지사장은 이러한 보안 정책 및 절차가 자신들의 지역에 규정될 수 있음에 책임을 가진다.

이러한 정책은 사무국의 승인이 이루어진 것이며 현재뿐만 아니라 미래의 모든 NCSA 직원에 적용되며 여기에서 직원은 정규직 및 비정규직, 그리고 학생 및 시간제 직원을 포함한다. 이는 개별 사용자 계약이 이루어지는 경우를 포함하는 NCSA의 HPC 자원의 방대한 사용자 범위를 의미하지 않는다. 이는 NCSA

네트워크 또는 NCSA 지적 재산에 속한 경우에 한하여 모든 NCSA의 장비 및 시설, 그리고 개인 장비의 사용에 적용된다.

이 정책은 Illinois 대학의 보안 정책을 대체하지 않으나 이를 보완할 수 있다. NCSA는 Illinois 대학의 한 분과이며 이는 궁극적으로 대학의 모든 정책 및 절차를 따른다. 만일, 대학의 정책과 NCSA의 정책이 충돌을 일으킨다면 대학의 정책이 우위에 있게 된다. 그러나 이러한 경우는 매우 제한적이며 대부분의 정책은 우선권을 가진다. 마찬가지로 이러한 정책은 특정 데이터 (예를 들면, 의료 기록)를 취급함에 있어서 형사상 또는 민사상의 법률 규정을 필요치 않는데 이는 훨씬 더 제한적이기 때문이다.

나아가 NCSA에서의 특정 과제 및 제휴는 별도의 보안이 요구될 수 있다. 예를 들면, IBM과의 Blue Waters 대용량 컴퓨팅 프로젝트의 경우는 별도의 계약을 통하여 추가적인 기밀 유지 보안이 이루어진다. 그러므로 이 프로젝트에 관여하는 직원은 일반적인 NCSA 정책 보다 더 엄격한 보안 정책이 적용되는 보안 수준을 준수하여야 한다.

일부 컴퓨터 시스템은 부가적인 물리적 보안을 필요로 하는데 여기에서의 정책은 정보 및 사이버 보안을 목적으로 한다. NCSA 보안 팀은 이러한 정보 및 사이버 보안의 책임을 가지며 보안의 구성은 행정 사무국의 관할권에 따라 이루어진다.

1.3. 관련 정책

Illinois 대학의 정보 기술 정책은 NCSA 정책에 적용하지 않는 약간의 추가적인 토픽과 더 세부적으로 일부를 다루고 있다.
이러한 정책은 또한 NCSA가 대학교와 한 계열인 것처럼 NCSA 직원에게도 적용된다. 토픽엔 포함되지만, 제한하지는 않는다:

- 소프트웨어 표절, 파일공유와 P2P 유틸리티
- 대역폭 사용
- 개인 식별 정보 처리
- 프라이버시 정책과 개인의 권리

2. 인식

개인 뿐만 아니라 물리적 대상과 정보에 대한 적정 수준의 보안을 제공하는 것이 NCSA의 보안 정책이다. 직원을 포함한 NCSA의 종사자들은 이러한 정책에 대한 문서를 숙지해야 하며 보안을 위한 절차를 인지해야 한다. 보안에 관련된 문제가 제기될 때 직원들은 감독관이나 지국장 또는 NCSA 보안 사무소로 보고해야 한다.

각각의 직원에게는 HR (Human Resource) 오리엔테이션 기간 동안 이러한 NCSA 보안 정책 및 절차 관련 문서를 제공한다. 이들 문서는 담당 직원들이 고용된 첫 번째 주 동안 감독관 또는 지국장과 함께 숙지될 수 있어야 한다. 담당 직원 개개인의 특정 영역에 대한 구체적인 절차와 함께 일반적인 정책 및 절차 등이 검토되어야 한다. 이러한 숙지 및 검토 작업은 문서의 모든 내용에 적용된다. 새로이 고용된 직원은 반드시 이러한 보안 정책에 대한 문서를 읽고 이해하여야 하며 이는 자신의 서명이 포함된 보안 인지의 문서로서 남겨져야 한다. 이러한 문서의 원본은 직원의 HR 폴더에 저장되어야 하며 다른 관련 전자 문서들은 HR 및 보안 팀이 열람 가능한 데이터 베이스에 저장된다.

모든 신규 직원들은 일차적으로 신입 직원 보안 훈련 과정에 참가해야 한다. 이러한 훈련 과정은 정기적으로 열리며 극히 일부의 자격을 갖춘 직원의 경우를 제외하고 적용된다. 훈련 과정의 일정 및 시간은 NCSA 보안 사무국으로부터 얻을 수 있다.

각각의 지사는 적어도 일년에 한 번 각 지사에 적용되는 보안 정책 및 절차에 대하여 교육을 실시해야 한다. 지사들은 보안에 관련된 시스템 및 활동 그리고 NCSA 직원들의 보안 정책 및 절차 이행에 대한 모니터를 정기적으로 수행하여야 한다. 이러한 제반 내용의 숙지 및 훈련을 통한 직원들의 보안 능력 향상에 대한 관리가 이루어져야 하며, 이를 통하여 절차 및 적정 수준의 보안 규정을 위한 노력을 이룰 수 있도록 한다. 아울러 지국장은 이러한 과정이 잘 이루어지고 있는지 확인하며 필요한 경우 조언을 할 수 있다.

독점적 정보는 명확하게 표기되어야 한다 (6.4절 참고). 이러한 외부적이고 눈에 띄는 표시는 직원들에게 보안의 중요성을 강조하는데 유용한 수단이 된다. 직원들은 충분한 수준의 보안의 인지 상태를 유지하기 위한 이러한 메커니즘을 가져야 한다.

감독관은 직원들의 수행 능력 평가가 끝났을 때 보안 절차 승인을 고려해야 한다. 보안 관련 문제는 HR에 의한 면접이 이루어진 후 관련 부서 담당자를 통하여 발표된다 (6.3절 참고).

3. 보증

적정 보안 수준의 정의 및 실행은 규정된 정책과 절차가 정상적으로 이행되는지에 대한 확인의 지속적 과정을 필요로 하며 이러한 정책 및 절차는 직원과 사용자 사이의 적절한 소통을 통하여 이루어진다. NCSA는 이러한 과정에 대하여 여러 조직적이고 운영적 측면을 통하여 보증을 하게 된다.

3.1. NCSA 보안 팀

보안 팀이라 불리는 NCSA의 전산 보안 팀은 보안 가이드 라인 설정 및 NCSA 컴퓨터 및 네트워크 환경의 통합을 도와준다. 보안 팀은 보안상의 취약성이나 사고를 추적하며 이의 해결을 위한 조처를 수행한다. 또한, 보안 팀은 사고 대처 및 보안 팀, IRST (Incident Response and Security Team)을 포함 한다 (세부 항목 규정을 참고).

3.2. 직원의 책임

각 업무 영역은 정해진 보안 정책 및 절차의 이행에 대한 책임을 위한 개별 담당자 및 구성원과 함께 지국장을 구성원으로 가진다. 지국장의 책임은 해당 업무 영역에서 직원들의 일일 업무를 총괄하고 유지하는 구체적인 절차 이행의 확인에 있다. 또한, 지국장은 보안 정책의 특정 절차 및 설명에 관련된 직원들의 질문에 대응을 하여야 한다.

담당 직원들은 각자의 영역에서 정해진 절차에 따라 업무를 수행을 하며 이에 대한 책임을 가진다. 또한, 정책에 따른 절차의 이행을 숙지해야 하는 책임이 있으며 이를 통하여 개별 직원은 특정 상황에 대하여 규정에 얽매이지 않는 합리적인 결정을 할 수 있게 된다. 그러나 후자의 경우 스스로의 결정에 대한 상황 (뒤에 설명)에 대한 보고의 책임이 뒤따르며 다른 직원에게 추후 참고를 위한 설명 절차가 요구된다. 각각의 직원은 보안 절차 이행에 있어서 알려진 또는 예상되는 문제 또는 인가되지 않은 사용자에 대한 민감한 정보의 노출을 보고해야 한다. 이러한 보고는 제 6.2절의 규정에 따라 NCSA IRST 팀에게 즉각적으로 이루어져야 한다.

이러한 문서의 규정에 따른 정책 및 절차의 이행에 있어서의 실수는 대학 및 NCSA 정책에 따라 징계 사유가 되며 해고의 징계에 이를 수 있다.

4. NCSA 시설의 물리적 보안

4.1. 물리적 보안

이번 장은 NCSA 보안 정책의 물리적 보안에 대하여 기술한다. 이 장의 모든 자료는 물리적 보안에 관련된 것이다. 전자 데이터 보안 및 지적 자산의 보안 문제도 궁극적으로 이러한 보안의 범주에 속한다. 물리적 보안은 자물쇠 및 잠금 장치와 같은 물리적 도구와 함께 건물 및 사무실 등의 보안을 포함한다. 물리적 보안은 전자 데이터 및 지적 자산과 관련된다. 컴퓨터에 대한 접근이나 종이 문서 등에 대한 접근은 전자 데이터의 보안 문제를 야기할 수 있게 된다. 물리적 보안은 여러 변수에 따라 달라질 수 있다. 건물의 경우 복도, 벽체, 지붕, 그리고 특히 창문 등의 요소가 보안에 중요한 영향을 준다. 창문의 경우 약 6인치 (약 15cm) 정도 열리게 되면 보안에 위험 요인이 되며 지상 층의 경우 더욱 취약하게 된다.

경보 및 다른 보안 시스템들은 건물 보안을 향상 시킬 수 있다. NCSA 건물의 일부 유형들은 출입문 감시 시스템이 있으며 움직임을 감지하여 경보를 울리는 시스템이 가동된다.

NCSA 건물의 경우 건물내의 장비 및 정보의 종류, 수량, 그리고 가치 등 중요한 보안 요소가 있다. 이러한 장비 및 정보의 가치가 클 수록 이에 대한 NCSA 보안을 파괴하려는 시도가 증가할 수 있다.

4.2. NCSA 건물 보안

2005년 9월 NCSA는 Illinois 대학의 두 건물 ACB(Advanced Computations Building)와 NCSA 빌딩이 입주하였다. Petascale Computing Facility는 2009년 공사 중이며 이 건물은 ACB을 대신하게 될 것이다. 이들 건물은 NCSA 물리적 보안에 직접적인 영향을 주었다. 이들 건물의 구체적인 보안 시스템 및 절차는 아래에 기술한다. NCSA 건물에 있어서의 공간 사용 및 건물 내부의 직원들은 사무국장의 지시에 따른다.

NCSA의 통상적인 근무 시간은 휴일을 제외하고 월요일부터 금요일까지, 오전 8시부터 오후 5시로 규정한다. 모든 대학 내의 건물들은 BSW (Building Service Workers)에 의해 청소가 이루어지며 F&S (Facilities and Services)에 의해 유지된다.

모든 대학 건물 들은 이러한 F&S, BSW, 그리고 관련 장비 등을 위한 공간을 두게 된다.

4.2.1. ACB

NCSA는 기계 설비 및 관리인을 위한 공간 이외의 나머지를 모두 ACB를 위하여 사용한다. ACB의 입구 및 컴퓨터실은 항상 잠겨 있어야 하며 출입을 위하여 키 카드 시스템을 적용한다. 비디오 카메라는 모든 입구에 설치되며 제어실에서 담당 직원에 의하여 감시가 이루어진다. 인터콤과 원격 잠금 장치가 주 출입구에 사용되며 이는 키 카드를 소지하지 않은 인가된 사람의 출입을 통제하기 위해 사용된다. ACB는 일반인에게 개방되지 않으며 직원에게는 일년, 일주일, 그리고 24 시간 내내 출입이 허용된다.

4.2.2. NCSA 빌딩

NCSA 빌딩은 대부분의 직원이 근무하는 건물이다. 북쪽과 남쪽의 출입문은 정규 근무 시간에 열려 있으며 근무 시간 이외의 출입에는 키 카드가 필요하다. 옆문은 잠겨 있으며 항상 키 카드를 사용하여 출입이 가능하다. 또한 NCSA 빌딩은 모든 출입문에 감시 카메라가 설치되어 있다.

4.3. 물리적 보안의 요건

건물의 모든 외부 출입문은 잠긴 상태로 유지되며 특별한 경우에 한하여 필요에 따라 개방된다. 출입문은 담당 직원의 출입 감시가 이루어지는 상황에 한하여 해당 출입문을 개방할 수 있다. 직원의 안내 없이는 누구든 건물이나 사무실에 접근 할 수 없으며 직원과의 친분을 통한 출입은 허용되지 않는다. 직원들은 인가되지 않은 사람의 NCSA 건물 또는 사무실의 접근을 허용해서는 안 된다. 의심이 가는 접근자 또는 직원의 신분증을 가지지 않은 사람을 발견하는 경우는 자신의 상급자 또는 지국장, 또는 대학의 경찰에게 보고 한다. 만일, 건물 내에서 잠금 장치 고장, 문이 열려 있는 경우, 또는 문을 열려고 하는 경우 및 위험 요소가 존재하는 경우는 반드시 건물 유지 보수 부서, 지국장, 또는 상급자에게 보고 한다.

개별 워크스테이션은 사용자의 사무실에 대한 물리적 보안의 대상이 된다. 사용자들은 반드시 자신들의 사무실이나 컴퓨터에 외부인이 접근 할 수 없도록 조치를 해야만 한다. 모든 사무실은 내부에 직원이 남아있지 않을 경우,

근거리에서 사무실을 주시 할 수 없는 경우 반드시 잠가야 한다. 사무실에 특별히 중요한 자료 (아래 참조) 근무 시간 중에 잠깐 자리를 떠날 때는 사무실을 잠그지 않아도 무방하다. 그러나 사무실에 직원이 남아있지 않을 경우 또는 사무실을 감시할 사람이 없을 경우 (개인의 소지품을 보호할 필요가 있을 경우) 언제나 모든 사무실 문을 잠가야 한다.

모든 컴퓨터실 및 통신실은 잠가야 하며, 시스템, 생산 서버 (세부 항목 규정을 참고), 그리고 관련 장비들은 특별히 고안된 컴퓨터실에 설치되어야 한다. 이러한 컴퓨터실들은 특별히 제어되는 장치로서 잠가져야 한다.

컴퓨터 및 다른 중요한 장비로 이루어진 실험실 및 교육장은 항상 잠가져야 하며 인가된 직원에게만 출입이 허용되어야 한다. NCSA 컴퓨터에 일반인의 접근이 허용되는 경우는 물리적 잠금 장치 및 로그온에 의한 보안이 이루어져야 한다.

기밀 및 중요한 정보는 보안이 이루어져야 하며 이들 정보는 NCSA의 다양한 사무실에서 사용된다. 이러한 정보는 근무 시간 혹은 근무 시간 이후에 사용자에 대한 제어가 어렵기 때문에 NCSA 직원들은 해당 사용자들에게 사무실을 비우는 경우 항상 사무실을 잠가서 보안 유지를 해야 함을 당부해야 한다.

사무실 및 건물의 여러 열쇠들은 NCSA 직원들에게 나누어지며 이들은 Keys and Keycard 정책 (Keys and Keycard 정책 참고)에 따라 관리된다. 열쇠는 직속 상급자에게 일정 양식을 통하여 요청 할 수 있으며 지국장의 승인으로 지급이 이루어진다. 마스터 키는 일반적으로 정규직 관리자에게만 주어지며 이는 사무국장의 승인에 따라 지급된다. 보안 팀은 설비 담당 부서의 지국장과 함께 마스터 키를 소지하고 있는 직원들을 정기적으로 관리 한다.

고용된 직원의 사무실에 있는 장비는 해당 사용자인 고용인에 관리의 책임이 있다. 만일 사용 중인 장비가 이동되거나, 고장, 교체, 또는 업그레이드 되면 Shipping and Receiving 부서에 이를 반드시 보고한다.

지정 장소 이외에서 NCSA 장비를 사용하는 직원은 해당 장비의 물리적 보안에 대한 책임을 가진다. NCSA의 모든 장비가 지정된 장소를 벗어나 사용되는 경우는 감독자의 승인이 필요하며 Shipping and Receiving 부서에 'Off-Site Equipment Usage Authorization' 양식을 이용하여 승인을 얻어야 한다. 이러한 장비는 Shipping and Receiving 부서를 통하여 연중 재고가 확인되어야 하며 관리가 이루어져야 한다.

만일 NCSA에 귀속된 장비를 잃어버리는 경우는 e-mail을 통하여 즉시 재고 관리 부서로 보고한다.

만일 NCSA에 귀속된 장비의 도난이 발생된 경우는 경찰에 신고가 되어야 하며, 또는 대학 경찰에 전화하여 신고할 수 있다. 만일 도난 장비가 $300을 초과하는 경우는 다른 번호로 신고 한다. 경찰에 신고가 이루어지면 신고 양식 한 부를 Shipping and Receiving 부서에 보내어 재고 관리에 적용될 수 있도록 한다.

만일 NCSA에 귀속된 장비가 파손되어 수리가 필요한 경우는 직속 상관에게 보고 한다.
장비가 폐기 (잉여/고장)될 경우는 Shipping and Receiving 부서로 보낸다. 장비의 폐기가 이루어지기 전에 내장된 하드디스크는 수거하여 'Illinois Data Security on State Computers Act'에 따른 데이터 제거 작업 과정을 거쳐 폐기한다. 이러한 데이터 제거 작업은 'Illinois Public Act 093-0306'을 따르며 가장 확실한 방법을 적용하여 제거 한다.

개인간 또는 그룹 내에서의 장비 교환이 이루어지는 경우는 중요한 데이터 (원본 또는 생성 자료)가 있을 수 있으므로 하드디스크의 데이터 제거 과정을 거친다. 이러한 데이터 제거는 앞에서 언급한 규정 및 방법을 따른다.

5. 네트워크 및 시스템 보안

네트워크 보안은 네트워크를 통하여 이동되는 데이터의 보안 사고 (서비스의 거부, 비허가된 접속 등)와 함께 이들 데이터의 보존성 및 기밀성이 주요 대상이 된다.

5.1. NCSA에 대한 인터넷 접속

NCSA의 인터넷 연결은 NCSA의 자원에 대한 높은 성능의 접속을 제공한다. 인터넷 접속은 NCSA 접속으로부터의 공격을 방지하거나 NCSA 자체의 문제를 해결하기 위한 패킷 필터 및 "방화벽" 메커니즘을 갖는 일련의 라우터 세트를 통하여 이루어진다. NCSA 필터링 또는 방화벽 메커니즘의 구체적인 내용은 NCSA 네트워크 그룹 또는 보안 팀으로부터 얻을 수 있다.

5.2. NCSA 인터넷 네트워크

NCSA는 여러 건물 사이의 연결을 위하여 백본 네트워크를 운영한다. 백본 네트워크에 대한 모든 연결은 각 건물에 설치된 NCSA 보안 네트워크 사무실내에 네트워크 종료 지점을 가지며, 네트워크의 기본 요소 (라우터, 스위치, 등) 및 보안 장비 (모니터)를 제외하고 어떤 컴퓨팅 장비도 백본에 직접 연결될 수 없다.

NCSA 또는 대학 소유의 장비 외에 사용자 감독관에 의한 승인이 있는 사용자만이 NCSA 네트워크에 접속이 가능하다. 이러한 연결 장비는 개인의 노트북 컴퓨터, PDA, 그리고 무선 접속 포인트를 포괄한다.

NCSA 내부 네트워크에 대한 무선 접속은 NCSA의 무선 접속 포인트를 통하여 이루어진다. 감독관이나 지국장의 승인, 또는 네트워크 엔지니어링 감독관의 허가 없이는 NCSA 네트워크 접속이 허용되지 않는다.

5.3. 컴퓨터 시스템 보안

NCSA 관련된 컴퓨팅 보안에는 첫째, 운영 체계 보안 둘째, 사용자 데이터 보안의 두 가지 유형이 존재한다. 이러한 두 가지 유형의 보안이 사용자와 NCSA 직원 사이에 존재하며 각각의 책임 한계가 존재하며 양자는 모두 보안 환경의 유지를 위하여 노력을 기울여야 한다.

운영 체계 보안의 목적은 첫째 승인되지 않은 사용자의 접근 방지, 둘째 승인되지 않은 데이터에 대한 접속을 시도하는 사용자의 차단, 셋째 컴퓨터 자원의 승인되지 않은 사용의 방지, 넷째 시스템의 가용성 유지, 그리고 마지막으로 승인된 사용에 있어서의 시스템 수준 변동에 따른 오류의 방지와 같은 다섯 가지 역할에 있다.

운영 체계 환경에 대한 보안은 중앙에서 관리되는 NCSA 시스템 관리 직원, 시스템 관리에 종사하는 NCSA 직원 및 연구원, 그리고 NCSA 운영 체계의 공급자(밴더)를 중심으로 이루어진다.

모든 장비의 관리자들은 자신들이 관리하는 장비를 가장 최신의 운영 체계로 업데이트한 상태를 유지하여야 하며, 불필요한 모든 서비스는 제거되어야 한다. 시스템 스캔은 모든 NCSA 장비의 취약점에 대하여 적용되고 이는 보안 팀에 의하여 이루어지며 관리자는 이러한 취약점에 대한 특별 패치를 설치할 수 있도록 지시한다 (제 5.8절 참고).

기계 운전 생산 서비스 (즉, 웹, e-메일, 데이터베이스, 등)에 적용되는 장비는 정해진 사무실에 설치되어야 한다 (세부 항목 규정을 참고).

윈도우를 운영하는 관리자는 NCSA에서 승인한 바이러스 방지 패키지 또는 NCSA 보안 팀에서 승인한 다른 종류의 패키지를 설치하고 운영하여야 한다. 이는 구매자의 요청 및 환경에 따라 업데이트 되어야 한다.

개별적인 직원들은 자신들의 상급자의 승인에 따른 시스템을 통하여 보안을 유지하여야 하지만 이들 개별 직원들은 자신들의 보안 유지 결여에 따른 문제에 전적으로 책임을 져야 한다. 학생들의 장비의 경우는 학생 사용자의 직속 상급자에게 보안 유지의 책임이 있다. 시스템의 관리자는 자신이 관리하는 시스템 자체로부터의 문제를 포함하여 다른 유형의 사고가 발생할 때 NCSA 보안 팀에게 반드시 보고를 이행하여야 한다.

만일 시스템의 장비가 문제가 생길 경우는 NCSA 보안 팀의 담당자를 통하여 해당 장비를 네트워크로부터 분리할 수 있다.

만일 개인 사용자가 자신의 전자 업무 환경 (즉, 계정 또는 자신의 시스템)에 문제가 있거나 의심이 가는 문제가 발생한 경우는 즉각 접속을 멈추고 (그러나 전원을 끌 필요는 없다) NCSA 보안팀에 연락하며, NCSA 보안팀은 NCSA Help Desk 또는 e-메일을 통하여 연결이 가능하다.

NCSA 컴퓨팅 시스템은 NCSA의 지능 환경에 맞는 시스템 선택을 위한 여러 과학자들의 협력으로 설계되었다. NCSA 정책은 사용자들이 데이터 공유에 있어서의 의사 결정 및 사용자 스스로에 의한 결정을 가능하게 하는 도구를 제공한다. 이러한 환경에서 사용자들은 자신들의 데이터에 대한 보안을 위하여 다양한 노력과 방법을 동원할 수 있다.

5.4. 계정 보안

NCSA 자원에 대한 모든 계정은 계정의 실행 이전에 NCSA의 규정에 따른 승인 절차가 필요하며, 자체 계정 관리 시스템에 있어서 만일 사용자가 NCSA 공용 자원에 대한 계정을 가지고 있다면 이는 로컬 시스템에 추가 등록이 요구된다. 그러나 시스템에서의 사용자 계정 관리 책임은 관리자의 영역이며 이들의 관리 책임은 NCSA에 의하여 승인된다.

계정은 인가된 개별 사용자에 의하여 사용될 수 있으며 이는 다른 사람과 공유될 수 없다. 비밀번호 및 개인 키는 어느 누구와도 공유될 수 없다 (이는 감독관, 동료, 그리고 배우자를 포괄한다).

사용자는 자신들의 계정과 관련된 개인 키의 보안을 반드시 유지해야 하며, 개인 키는 SSH 또는 PKI 인증과 같은 프로그램을 통하여 사용될 수 있다. 오랜 기간 사용이 유지되는 개인 키는 비밀번호에 의하여 보안이 이루어지며 소유자 자신만이 읽을 수 있는 파일로 저장된다. 사용자는 이러한 파일에 접속하기 위하여 반드시 비밀번호를 사용하며 빈칸이나 비어있는 비밀번호를 사용할 수 없다. NCSA는 일주일 정도의 사용 기간을 가지는 단기간의 개인 키를 허용하기도 한다. 만일 NCSA 계정과 관련된 개인 키에 문제가 생겼다고 의심되면 NCSA 보안팀에 즉각 연락하여야 한다. 이러한 문제에 대한 기술은 제 6.2절을 참고 한다.

기존의 비밀번호와 함께 새로운 계정의 정보는 사용자에게 메일로 고지되며 이에 대한 문서는 이후의 자료를 위하여 저장된다. 비밀번호를 잊은 사용자를 위한 안내를 위한 정보도 이러한 파일에 포함되며, 사용자는 초기 로그인 과정에서 자신의 비밀번호를 설정해야 한다. 만일 계정이 생성된 후 30일 이내에 비밀번호가 설정되지 않으면 이 계정은 잠금 상태로 지정된다.

사용자 스스로 관리가 이루어지는 시스템의 경우도 이와 같은 계정 및 비밀번호 적용이 이루어진다.

NCSA 보안 담당 직원은 불안전한 비밀번호의 색출을 위하여 비밀번호 파일을 열람할 수 있으며, 할당된 시스템의 계정은 분배 과정을 통하여 중앙 관리

방식으로 유지된다. 이 과정은 정기적으로 유효한 계정을 확인하며 문제가 되는 계정을 찾아낸다.

시스템 관리자 계정은 엄격한 승인을 통하여 관리되며, 이러한 계정에 대한 접근은 중앙 관리 방식으로 자주 관리되며 감시된다.

NCSA는 분명한 문자 형태의 비밀번호 (암호화되지 않은 고정 비밀번호)를 통한 어떠한 원격 시스템에 대한 접근을 허용하지 않는다. 커베로스, SSH, 또는 다른 보안 방식이 반드시 사용되어야 한다.

직원의 계정은 고용 관계가 끝나면서 승인 상태가 취소된다. 대용량 저장 (mss)에 대한 접근은 계정 상실 후 4개월 동안 유효하다. 이러한 접근 시간은 해당 감독관 또는 감독 사무국에 의한 승인 요청이 있을 경우를 제외하고 할당된 또는 생산 시스템의 경우에 적용된다.

5.5. 파일 시스템 보안

할당된 모든 파일 시스템과 생산 시스템은 사용자의 수정으로부터 보호되며 수정 여부를 정기적으로 점검된다. 감시 프로그램을 통하여 사용자 또는 승인되지 않은 것에 대한 변경 여부도 점검 한다.

원격지에서 접근이 가능한 파일 시스템 (예를 들어, NFS 및 윈도우 공유 등)은 NCSA 관리를 받는 네트워크에 위치한 시스템으로의 전송이 가능하며 이러한 관리 범위 밖의 시스템으로의 유출은 허용되지 않는다. 이러한 규칙의 예외 조항은 NCSA 보안 팀의 승인을 받는 경우에 한하며 이러한 승인은 e-메일을 통하여 가능하다.

이러한 보안에 있어서 시스템 또는 보안 관리자는 문제를 해결하기 위하여 해당 파일 및 디렉토리에 접근이 가능하다.

5.6. 데이터 분류

서로 다른 수준의 보안 등급이 요구되는 데이터 분류는 다음의 세 가지 등급으로 구분된다.

- **공개 수준** – 정보를 자유로이 공개 할 수 있는 수준

- **기밀 수준** – 데이터의 소유주가 공개를 원치 않는 기밀 수준 또는 공개될 경우 손실을 초래하여 NCSA에 대하여도 기밀이 필요한 수준

- **사적 소유 또는 유출 제한 (높은 위험) 수준** – 공개될 경우 법적인 제재를 받거나 재정적인 책임이 필요한 수준의 정보. 이러한 수준의 데이터는 연방 또는 주정부 수준의 법적 제재가 따르며 이에 해당되는 데이터는 FERPA, HIPAA, 또는 Data Protection Act, EAR 99, ITAR, 그리고 계약, 비공개 형식 문서, 소프트웨어, 문서, 그리고 그래픽과 같은 특정 사용자 데이터 등이다. 이러한 데이터는 무형의 자산으로서 사상 및 이념, 문서, 생성된 데이터, 그리고 모든 형태의 그래픽 정보를 포함한다. 임금 명부, 개인적 정보, 그리고 재정 정보 등은 사적인 정보이므로 이 등급의 수준에 포함된다.

이들 등급은 대학의 정보 보안 정책의 'Data Classification Policy'의 일부로 시행된다.

이러한 데이터 분류의 수행 절차는 본 문서를 통하여 고지된다.

5.7. 데이터 보전 (백업)

백업은 모든 제품, 데스크 탑, 그리고 노트북 컴퓨터에 대하여 주기적으로 이루어진다. 이러한 백업은 하드웨어의 문제 또는 고장에 대비하기 위한 방법의 하나로서 데이터의 보전성을 유지한다. 일반적인 데이터 영역 또는 일시적인 데이터 영역은 백업되지 않는데 이들 데이터는 매우 용량이 크고 일시적인 저장 영역이므로 대상에서 제외된다. 복제 백업 테이프는 NCSA의 별도의 장소에 보관되며, 테이프를 통한 백업은 백업 시점으로부터 90일 동안 보관되며 이 기간 이후에는 다른 백업을 위하여 테이프가 재활용된다.

5.8. 시스템 관리 보안의 감시

컴퓨터 시스템에 대한 보안은 매우 복잡한 문제가 된다. 다른 업무의 경우 자동화가 가능하지만 보안의 기본 수준의 보안은 시스템에 대한 이해와 책임을 수반하는 관리자에 의해서 실현된다. 관리자의 수와 보안 유지에 소요되는 시간은 대상 시스템에 따라 다르게 된다. 심각한 수준의 보안 문제가 발생하는 경우 보안팀의 접근 방식은 의심이 가는 대상을 제외하고 가능한 많은 데이터를 수집하는 것으로 시작된다.

로그 파일 및 매뉴얼에 따른 감시는 자동화된 절차가 사용된다.

보안 스캔은 NCSA 보안 팀에 의하여 주지적으로 이루어진다. 이러한 스캔은 시스템의 안정성을 평가하며 다른 시스템의 노출 상태 등을 검사한다. 관리자는 시스템의 문제를 공지해야 하며 최상의 보안 상태가 유지될 수 있도록 조언을 한다. 이러한 스캔은 최소 6개월 동안 유지되어야 한다. 보안 팀은 이러한 스캔으로부터 발견한 모든 문제들을 공지한다.

호스트 및 네트워크 침투 감지 시스템은 보안 팀에 의하여 사용되며 시스템에 대한 침투 및 손상을 감시한다. 시스템에 대한 침투가 발생한 경우 보안 팀은 이러한 시점에 대한 부가적인 감시를 실행한다.

5.9. 전자 메일

생산성 도구의 하나로서 NCSA는 전자 메일의 사용을 권장한다. 그러나 이러한 전자 메일을 포함하여 인터넷에의 접속은 이러한 사용자들이 위험에 노출될 수 있게 한다. NCSA는 이러한 개별 사용자들의 전자 메일 사용에 따른 수신, 다운로드, 불순한 의도를 가진 내용 또는 소프트웨어 또는 해로운 소프트웨어 (컴퓨터 바이러스 등)에 대한 책임을 가지지 않는다.
NCSA는 사적인 개인 메일의 사용에 대한 보안의 보장을 하지 않는다. 전자 메일은 사용하는 기술 환경에 따라 다른 사람이 열어 볼 수 있으며 인쇄 될 수 있고 저장 될 수 있다. 또한, 의도적으로 전자 메일에 접근이 가능하다. 전자 메일은 시스템 내에서 백업될 수 있으며 나중에 다시 열람이 가능하고 전통적인 방식의 편지처럼 폐기가 가능하다. 담당 직원은 중요한 메일의 전송에 있어서 그 내용이 보호되지 않은 상태로 보내지는지를 감시하여야 한다.

사용자는 첫 번째 다른 전자 메일 서비스로부터 (예를 들어, POP) NCSA 전자 메일에 접속할 수 없으며, 두 번째 자신의 NCSA 전자 메일을 'CITES Express Mail'을 제외한 다른 메일 서비스에 대한 접속을 금지한다. Gmail과 같은 다른 전자 메일 서비스를 사용하여 POP 또는 다른 프로토콜을 경유한 NCSA의 계정 접근은 본질적인 불안정성 때문에 NCSA 커베로스 비밀번호를 저장하기 위하여 별도의 도구가 필요한데 이러한 비밀번호 공유는 여러 이유에 기인하여 본 보안 정책에서 금지된다. 사용자의 NCSA 메일을 Blackberry 또는 Gmail과 같은 서비스를 이용하기에 편리함이 있을지라도 이는 결과적으로 NCSA의 보안 범위를 벗어날 수 있다. 예를 들면, 만일 중요한 메일이 암호화되지 않은 상태로 보내지는 일이 생긴다면 이러한 메일은 추적이 어려우며 삭제할 방법이 없게 된다. 결국, 제 삼 (third party)의 서비스 제공자에 의한 메일 서비스에 대한 보안 메커니즘 및 사적 보호는 보장될 수 없게 된다.

이러한 보안에 있어서 전자 메일 관리자는 문제 해결을 위하여 사용자의 우편함을 점검할 필요가 있다. 그러나 이러한 점검은 문제 해결을 위한 꼭 필요한 경우가 아니면 실행될 수 없다.

전자 메일은 바이러스, 스팸, 또는 부적절한 소프트웨어 점검을 위한 NCSA 메일 서버를 경유하면서 스캔이 이루어진다. 스캔은 사용자의 요청이 있을 경우 이 시스템을 거치면서 자동으로 문제가 발견되며 이들 문제를 막을 수 있다. 이러한 서비스의 요청은 메일을 통하여 신청이 가능하다.

NCSA 직원이 프로젝트 관리자 또는 소유자의 승인을 얻지 않고 중요한 정보 (세부 항목 규정을 참고)의 전자 메일을 전송하는 것은 NCSA의 보안 정책에 위배된다. 그러나 이러한 정보의 소유자는 자신의 정보에 대한 위험에 대한 전자 메일 사용을 선택할 수 있다. 암호화의 기술은 이러한 중요한 정보의 전송에 도움을 준다.

의도적인 바이러스, 연쇄 메일, 장난 메일, 또는 다른 부정한 의도의 전송을 위한 전자 메일은 금지된다.

5.10. 인터넷 사용

NCSA 자원 (즉, 컴퓨터 또는 네트워크)에 대한 손상을 위한 어떠한 시도도 엄격히 금지된다. 나아가 NCSA의 내부 네트워크 또는 인터넷에서의 바이러스 또는 부정한 코드의 유포도 엄격히 금지된다. 유일한 예외의 경우는 NCSA 보안 팀의 승인이 이루어진 경우 (즉, 침투 시험) 또는 지국장의 승인 (적절한 안전 지침에 따르는 승인을 얻은 보안 연구 프로젝트)에 따른 연구 프로젝트에 대하여 적용된다. NCSA 전자 보안 시스템의 파괴나 침투, 또는 네트워크 기반의 보안 메커니즘의 우회 접근 역시 금지된다.

음란물, 선정적 또는 인종적 자료, 또는 불법적인 정보 및 그래픽을 포함한 제한적인 자료의 취득, 공유, 저장, 열람, 전자 메일 전송, 그리고 다운로드 등의 NCSA 또는 대학의 보안 정책에 위배되는 행위는 금지된다.

NCSA 자원을 광고 또는 상업적 목적으로의 서비스는 엄격히 금지된다. NCSA의 자원은 NCSA와 관련되지 않은 프로젝트의 인터넷 도메인으로서의 호스트로서 사용될 수 없다. NCSA 감독 사무국은 이러한 부적절한 용도의 모든 자원의 사용에 대하여 정당한 방법 및 목적이 아니라 판단이 되면 이러한 서버로부터 언제든 임의로 제거할 수 있는 권리가 있다.

6. 절차

6.1. 정책 및 절차의 수립

각 지국장은 여기에서 언급하지 않은 보안 정책 및 절차에 대하여 이의 특정 보안 분야에 대한 적용 및 절차의 수립에 책임을 가진다. 복수의 지부를 갖는 NCSA의 경우 지국장의 책임은 이러한 특정 보안 정책 및 절차의 이행을 위한 개인 또는 동료와 함께 책임을 가진다.

지국장은 자신의 지역에서 이러한 특정 보안 정책 및 절차의 이행에 대한 분석 및 평가를 위한 내부 및 외부로부터의 평가 및 감사 등에 참여하게 된다. 또한 지국장은 필요한 경우 자신의 지역에서 NCSA 정책 및 절차의 이행 유지 위한 보고 체계를 구성할 수 있다.

지부 사무국은 정책 및 절차의 변화에 대처하는 책임을 가지며, 만일 현재의 정책 및 절차에 변화가 필요하다면 현재의 정책 및 절차에 대한 년간 평가를 담은 보고서는 반드시 작성되어야 한다. 변화에 대한 요구는 이러한 변화의 실현 가능성 및 제안된 변화에 따른 비용 등을 보고하게 될 담당 지국장에 의하여 평가될 수 있다. NCSA에서의 모든 변화는 지국장에 의하여 승인된다. 일반적으로 새로운 정책 및 절차는 특정 절차의 이행에 책임을 지는 직원과 함께 감독 사무국에 의하여 평가되는 문서의 형태로 만들어진다. 새로운 정책 및 절차는 감독 사무국의 판단에 의하여 이와 같은 문서로 만들어진다. NCSA 직원 및 'Private Sector Partners'는 변화에 관련된 이러한 문서가 작성되었음을 고지 받는다.

6.2. 사건의 보고

보안 관련 사고 (세부 항목 규정을 참고)에 대한 관심을 갖는 것은 모든 직원들의 책임이며 이러한 사고를 발견하면 즉시 NCSA 사고 대응 및 보안 팀 (NCSA IRST)에 신고하여야 한다. IRST는 HelpDesk 또는 전화를 통하여 24시간 연결이 가능하다. 신고가 접수되면 IRST는 즉각 해당 사고를 조사하고 필요한 경우 해당 개인 또는 부서 등에 알리고 해결 방안을 제시한다.

6.3. 예외 과정

보안에 있어서 우리의 환경을 모두 예상하는 것은 현실적으로 가능한 일이 아니며 이러한 보안 정책에 예외 (일시적 또는 영구적)가 존재하고 이러한 예외에 대하여 일일이 정책을 바꿀 필요는 없게 된다. 이와 같은 정책의 예외에 대한 요청 과정은 본 문서의 변경 (제 6.1절 참고)의 과정과 동일하며 이러한 예외는 감독 사무국 및 보안 사무국의 승인을 반드시 얻어야 한다. 보안 사무국은 현재의 예외 조항에 대한 모든 경우들을 인지하고 있어야 한다.

6.4. 보안 이행 계획

지국장은 자신의 지부에 있는 감독관과 보안 정책 및 절차에 대한 의견을 교환하여야 하며, 또한 감독관으로부터 보안 정책의 이행 절차에 대한 의견을 들어야 한다. 지국장와 해당 감독관은 정책과 절차에 대한 검토를 수행하여야 하며 이의 변경 및 개선에 대하여 해당 감독 사무국과 협의를 하여야 한다. 모든 보안 관련 침해 및 위반 상황은 감독 사무국 및 보안 사무국에 보고되어야 한다. 아울러 감독 사무국 및 보안 사무국은 이러한 문제의 해결을 시도한다.

다음은 문제 해결을 위한 규정 절차 및 책임을 나타낸다.

- 지국장은 감독관 및 담당 직원과 보안 일반에 대한 문제를 논의하여야 한다.

- 지부 규정의 가이드라인은 해당 지역에 적합한 물리적 보안 및 컴퓨팅 보안 활동을 위하여 규정되어야 한다.

- 감독관은 자신의 관할 직원 및 보안 정책 그리고 절차에 대하여 항상 관심을 가져야 하며 이들의 영역에 대한 보안에 책임을 가진다.

- 감독관은 새로운 고용인에 대하여 NCSA 보안 정책 및 절차에 대하여 논의할 준비를 하고 있어야 한다. 새로이 고용된 사람은 감독관이 제공한 보안 정책 및 절차에 대한 문서를 읽고 숙지해야 하며 의문이 있을 경우 자신의 감독관에게 질문을 하여야 한다. 감독관은 각각의 고용인에 대하여 이들이 해당 문서를 이해하고 있는지 점검해야 하며 각자의 역할과 책임에 대하여 알려주어야 한다. 이러한 절차는 고용인의 전자 서명이 첨부된 전자 보안 승인 문서 양식을 통하여 작성되며 이는 HR에 고지된다.

- 비밀 유지 계약 (NDA, Non-Disclosure Agreement)에 따른 직원에 대하여 감독관은 이러한 계약의 속성 및 목적을 분명히 이해할 수 있도록 조언을 한다. 어느 누구든 서명이 첨부된 보안 승인 양식을 통하지 않고는 NDA가

요구되는 어떠한 프로젝트에 동참하는 것이 허용되지 않으며 프로젝트 규정 NDA는 HR의 파일에 등록된다.

- HR 직원은 NCSA에서 퇴사하는 해당 직원의 마지막 근무일 이전에 면담을 해야 한다. 이 면담은 해당 직원의 키 및 키 카드 등의 회수를 포함하며 만일 비밀 유지 계약을 한 경우라면 해당 계약 조건에 대한 확인을 점검하는 과정이 포함된다. 이러한 면담에 따라 해당 직원이 특정 자료를 소지하고 있거나 이를 NCSA 밖으로 유출할 의도가 있는지를 확인하게 된다. 직원이 퇴사하는 경우는 퇴사 양식에 따라 기록이 남겨지며 이는 HR 부서에 파일로 기록된다.

- 직원에 대한 보안 교육은 일정한 일정에 따라 정례화 된다.

- 직원들은 방문자들에 대하여 NCSA의 보안 정책 및 절차가 적절히 적용되고 있는지의 여부를 생각해야 한다. 방문자에 대하여는 방문자 패스, 키 또는 키 카드가 부여되며 방문을 마치는 경우 이를 회수한다.

6.5. 프로젝트 보안 절차

본 장은 사적인 자료 또는 민감한 데이터가 포함된 프로젝트에 관련된 보안 정책 및 절차에 대하여 기술한다. 이러한 경우의 가장 대표적인 프로젝트는 사적인 정보를 포함하는 'Private Sector Partner' 이며 이에 해당되는 모든 프로젝트는 관련 연구원에 대하여 적정 보안 수준이 요구된다. 여기에서의 연구원은 'Private Sector Partner'의 일원이든 아니든 "참여자" 로서 여겨진다.

프로젝트는 목표를 위하여 NCSA 직원과 함께 하는 공동의 활동 및 작업을 의미하며, 이러한 프로젝트는 문서 및 오디오, 비디오 자료를 포함하여 계획, 데이터 전송, 처리 또는 기록, 소프트웨어 개발, 하드웨어 개발, 그리고 보고를 포괄한다. 또한 프로젝트는 NCSA 또는 대학내의 다양한 부서의 사람들을 포괄한다. 프로젝트에 대한 책임을 가지는 지국장은 이러한 프로젝트의 수행에 대한 전반적인 조율에 대한 책임을 가진다. 'Private Sector Partner'를 포함하는 프로젝트에 있어서 지국장의 가장 중요한 점은 프로젝트 이행에 대한 점검에 있으며 특히 사적인 정보와 관련된 문제의 감독에 있다.

6.5.1. 계획

사적인 정보가 논의되는 프로젝트에 있어서 해당 정보를 소유하고 있는 공동 참여자는 모든 해당 정보에 대하여 분명하고 정확한 고지가 이루어져야 한다. 이는 문서로 작성되어 NCSA와 참여자 사이의 계약 (CA, Contractive Agreement) (세부 항목 규정을 참고)으로 규정되어야 한다.

NDA를 요구하는 모든 프로젝트는 공동 참여자와의 CA가 필요하며 이를 통하여 프로젝트가 실행된다. CA는 NDA에 서명이 요구되는 프로젝트에 참여하는 모든 참가자의 목록을 포함한다. 이러한 CA는 최소 한 부를 복사하여 프로젝트 PI (Principal Investigator) 및 NCSA 보안 사무국에 보관한다. NDA의 최소한의 복사본은 프로젝트의 PI와 함께 보관된다.

프로젝트를 위한 NCSA PI는 모든 NCSA 직원에 대한 서명이 첨부된 보안 관련 서류 (즉, NDA)를 확인할 책임을 가지며 해당 프로젝트에서의 보안에 대한 책임이 있다. PI는 CA에 해당되는 고용인들에 대한 서류 또는 NDA에 따르는 모든 고용인들에 대한 자료를 요청할 수 있다.

어떠한 NCSA 사용자도 NDA의 서명 없이는 사적 정보에 접근 할 수 없으며 이러한 정보 소유자가 등재된 목록에 접근할 수 없다.

보안의 계획은 프로젝트에 맞는 보안이 어떤 것인지 결정하는 것을 포함하며 이에 따른 절차는 아래와 같다.

1. 참여자의 요구가 있을 경우 프로젝트에 코드 이름이나 번호가 붙여질 수 있다. 이러한 코드는 프로젝트의 내부 및 외부의 통신, 계획 도구, 그리고 문서 등에 사용될 수 있으며 이를 통하여 프로젝트를 규정하거나 활동을 점검 할 수 있다. 어떠한 NCSA의 계획 또는 문서 작성의 경우도 연구의 특징 또는 일반 분야의 일부를 반영 및 암시하는 내용을 포함할 수 없다.

2. 프로젝트 참여자는 CA에 등록되어야 한다. NCSA, 공동 참여자, 그리고 관련 인력들은 이러한 목록에 포함된다. 또한, 이러한 목록은 사유 정보 등에 접근할 수 있는 사용자들을 포함되며 이 목록은 참여자와 NCSA 사이의 동의 및 서명을 통해서만 변경이 가능하다. 그리고 이 목록은 프로젝트의 진행이 이루어지는 동안 참여자의 이동이나 프로젝트 이탈이 있을 경우 반드시 수정이 이루어져야 한다. 이 목록에 등재된 참가자만이 모든 형태의 민감한 정보에 접근이 가능하다. 접근이 제한된 모든 자료들은 이러한 목록에 등재된 사람 이외의 허용을 불허한다.

3. 프로젝트에 관련된 보안 및 보안 유지를 위한 이행 절차에 대한 모든 문서는 보안이 유지되어야 한다. 또한, 비밀이 보장되거나 다른 보안 유지 대상은

서명이 이루어져야 하며 프로젝트에 관련된 모든 사적인 자료들도 보안이 유지 되어야 한다. 이러한 내용은 CA에 반드시 포함되어야 한다.

4. 프로젝트에 대한 어떠한 업무도 CA 및 관련 서류 (즉, NDA)에 서명이 이루어지기 전에 시작될 수 없다.

5. PI 및 참여자는 NCSA 보안 사무국에 귀속된 CA 관련 보안 내용을 고지한다.

6.5.2. 프로젝트 수행

프로젝트의 수행은 동료 참여자에 대한 파일, 문서, 데이터 (소프트웨어 포함), 그리고 하드웨어 또는 물리적 장비에 대한 접근을 포괄한다. 데이터는 중간 단계의 작업 또는 전송 가능한 형태의 자료를 생성하기 위한 소프트웨어 및 하드웨어를 통하여 분석되거나 변경될 수 있다. 보안 관련 문제는 참여자 파일 및 정보에 대한 접근을 포함하여 문서 및 데이터에 대한 접근을 포괄 한다. 데이터의 시각적 디스플레이는 컴퓨터의 모니터를 비롯하여 기타의 단말기를 통하여 이루어질 수 있다.

초기 데이터 획득 요건의 경우 이는 NCSA Data Receipt Form에 따라 문서화 될 수 있다. 이 문서 양식은 데이터의 속성 (사유권, 기밀성 등)을 규정할 수 있으며 데이터가 어떻게 받아질 수 있으며 저장을 위한 요건은 무엇 인지를 규정한다.

데이터 관리에 있어서의 NCSA 절차 및 승인은 데이터가 동료 참여자의 제어 영역으로부터 NCSA 제어 영역 (세부 항목 규정을 참고)으로의 전송이 시작되는 시점부터이다. NCSA는 NCSA에 의하여 운영되는 컴퓨터 시스템에 저장되는 데이터에 한하여 절차를 적용한다. 모든 프로젝트 기간 동안의 사적인 정보를 기록하는 컴퓨터의 디렉토리, 파일, 그리고 일시 저장 공간은 관리가 이루어지며 이들에 대한 접근은 인가된 사람으로 제한된다.

만일 사적인 정보가 물리적인 형태 (즉, CD, 테이프 등)으로 주어진다면 (이미 표시가 되지 않은 경우) "사적 정보" 라는 라벨을 붙인다. 전자 데이터의 라벨은 동료 참여자가 원하는 형식으로 지정한다. 기타 다른 라벨은 프로젝트에 준하여 붙인다. 예를 들면, "IBM 기밀 자료" 등과 같이 표기 한다.

프로젝트에 대한 감시는 NCSA 자원으로 저장되는 모든 사유 데이터를 갖는 모든 프로젝트에 적용된다. 이러한 감시는 CA에 대한 검토를 포함하여 NDA가 필요한 모든 개인, 데이터에 대한 개인의 접근, 그리고 다른 보안 관련 요건들에 대하여 적용된다.

참여자 데이터 및 연구 정보는 이들의 디스플레이 및 저장 매체에 대한 기록으로부터 반드시 보호되어야 한다. 필름, 비디오, 또는 다른 그래픽 매체에 대한 디스플레이 및 기록은 접근을 제한하는 환경에서 이루어져야 한다.

모든 생성된 데이터는 원본 데이터의 경우와 같은 취급이 이루어져야 한다.

CA에 대한 수정은 CA의 본래의 기한을 연장하는 경우 서명에 의하여 이루어질 수 있다.

프로젝트가 종료되면 인증된 동료 참여자의 대표가 민감한 정보의 제거에 대한 책임을 가진다. NCSA는 프로젝트에서의 어떠한 사적인 정보에 대하여도 소유하지 않는다. 만일 프로젝트의 종료 이후에 남아있는 사적인 정보가 발견된다면 이는 참여자가에 돌려주거나 파기 한다. NCSA 데이터 반출 양식 (Data Release Form)은 프로젝트의 종료에 따른 모든 프로젝트의 종료 양식에 적용된다. 이러한 데이터 반출 양식은 데이터의 제거 및 파기 방식을 규정한다. 데이터의 파기는 최근의 기술에 따른다.

일반적인 시스템의 백업은 시스템 및 시스템의 데이터에 대한 보전성을 보장하기 위한 것이다. 민감한 정보의 백업은 프로젝트의 기간을 초월하여 적용된다 (제 5.7절 참고).

6.6. 출판 및 발표

출판 및 발표는 CA에서 규정한 의무 규정에 따라 제한된다. 다음의 제 7.2.5절에서 PSP 참여자에 관련된 특정 출판 및 발표에 대한 규정을 기술한다.

6.7. 저작권 및 발간

일반적 기준에서의 아주 중요한 사적 자료 및 높은 보안 수준에 있어 NCSA 직원은 별도의 요청이 없는 한 특별한 보안 및 절차를 이행하지 않아도 된다. 이러한 고도의 중요 정보에 대한 보안 요구 및 특별한 정도의 보안 수준 요청은 해당 정보의 소유주의 요청 의지에 달려 있다. 이러한 특별 요청이 있을 경우는 별도의 문서 및 서명이 첨부된 양식으로 이행된다.

저작권은 동료 참여자가 제공하는 문서 또는 그래픽 자료가 NCSA에 의하여 전자 데이터로 발간되기 전에 확인이 이루어져야 한다. 필요한 경우 (즉, 이러한 자료가

NCSA에 귀속되지 않거나 공개 도메인에 노출도지 않기를 원하면) 이러한 자료는 NCSA에 귀속되어 사용되기 전에 저작권으로 보호될 수 있다.

이에 관련된 내용은 대학에서 규정한 "저작권 정책 및 발간"을 참고 한다.

6.8. 회보 및 공개 정보 그리고 기술 자료

담당 직원은 회보 및 기타 공개 자료에 대하여 앞에서 언급한 절차에 따른 문제가 없는지 확인하여야 한다. 또한 동료 참여자는 이러한 자료에 문제가 없는지에 대한 책임이 있으며 이에 대하여 NCSA에 문서로 보고 하거나 만일 이러한 자료 및 정보가 회보, 기사, 언론 등에 노출된 경우를 대비하여 시험 발간 동안 문제를 확인하여야 한다.

아울러 담당 직원은 다음의 절차를 이행한다.

- 내부 NCSA 자원으로부터 획득한 자료의 발간: 이러한 자료가 발간되기 전에 저작권 지정이 필요한지에 대하여 NCSA 직원에 의한 확인이 필요하다.

- NCSA에 귀속되지 않은 배경 또는 시각 자료: 담당 직원은 대상 자료가 발간되기 전에 해당 소유자와 함께 저작권의 문제가 없는지 확인한다. 해당 자료의 소유자는 문제 확인에 대하여 서명이 포함된 양식을 통하여 확인을 마친다. 이러한 자료의 배포에 문제가 있다면 자료의 소유자는 지정 양식을 통하여 이를 규정한다. 이러한 배포 제한에 대한 문서의 복사본은 모든 담당 직원에게 고지한다.

- 복사의 허용: 모든 직원은 상대 문서의 복사에 대한 승인 여부를 확인하여야 한다.

6.9. 고용인 퇴사 절차

고용인의 퇴사가 있을 경우 NCSA의 보안 및 지적 자산의 보호를 위하여 몇 가지 단계의 절차가 반드시 이행되어야 한다. 이러한 절차는 담당 관리자의 퇴사 처리 양식 기록을 통하여 자동으로 이루어지며 정규직, 비정규직, 그리고 학생 직원 등의 모든 고용인에 적용된다. 이러한 절차의 이행은 아래와 같다.

- 고용인이 사용하던 모든 장비는 해당 고용인이 퇴사 마지막 날 이전에 Shipping & Receiving 부서로 반납되어야 한다. 만일 해당 장비에 사적인 또는 기밀 정보가 포함된 경우는 장비가 다른 고용인에게 전해지기 전에

삭제 되어야 한다. Shipping & Receiving 부서는 장비의 재사용 이전에 모든 데이터를 제거하여야 한다.

- 계정의 무효화는 Kerberos 원칙을 포함하여 고용인이 퇴사하는 시점에서 가능한 빨리 이루어져야 한다. 그러나 공유 파일 시스템에 저장된 고용인의 파일은 1년 동안 백업으로 보관될 수 있다. 이러한 파일에는 AFS, MSS, 또는 전자 메일 서버의 내용 등이 포함된다.

    - 퇴사하는 직원은 NCSA와 일련의 관계가 남아있는 경우가 있는데 이는 연구 파트너 또는 다른 업무로서 이에 따른 계정이 필요하기도 하다. 이러한 경우의 고용인은 반드시 상이한 계정 이름을 부여 받아야 한다. 이는 시스템 관리자가 비공개 서버에 대한 접근에 대한 재량을 가지고 관리한다. 퇴사 고용인에 대한 계정 이름을 바꾸지 않을 경우 이러한 계정을 통하여 무의식적으로 여러 내부 시스템에 접근할 수 있게 된다. 이는 NCSA에서 관리되는 서버 및 서비스의 중앙 관리 방식을 벗어나는 결과를 보이게 된다. 이 결과는 전자 메일의 경우에서 이전에 사용하던 계정을 바꾸지 않은 경우에 동일하게 나타날 수 있다.

- 전자 메일 계정은 퇴사가 이루어짐과 동시에 무효화 되어야만 한다. 이러한 계정의 무효화는 퇴사자가 더 이상 NCSA의 전자 메일 서버를 통하여 자신의 전자 메일을 더 이상 확인할 수 없음을 의미한다. 그러나 퇴사한 고용인이 전자 메일 시스템에 접속할 수 없는 상황에서 전자 메일 관리자는 필요한 경우 당사자의 요청에 따라 당사자의 이전 주소에 대한 임의의 별칭 이름을 부여할 수 있다. 이 경우 전자 메일은 비 NCSA 계정을 통하여 메일이 전송된다.

    - 퇴사한 고용자의 계정을 NCSA 전자 메일 목록에서 즉각 삭제하는 것은 매우 중요하다. 이러한 즉각적인 삭제의 예외는 관리자의 요청에 의하여 보류될 수 있다. 또한, 퇴사한 고용인에 의하여 관리되던 전자 메일 목록은 무효화 되거나 다른 직원이 관리할 수 있어야 한다.

- 물리적인 키는 반드시 반납되어야 하며 키 카드에 의한 접근은 해당 직원의 마지막 근무일 이전에 중지되어야 한다.

7. 사적 영역 프로그램(PSP) 파트너

7.1. 사적 영역 프로그램 (PSP) 파트너

사적 영역 프로그램 (PSP) 파트너 (PSP 파트너 또는 파트너)는 파트너의 업무 특성 또는 파트너와의 특별한 관계에 기인한 특별한 보안 요건을 갖는 경우를 의미한다. 파트너에 의하여 이루어지는 대부분의 많은 연구는 매우 민감한 내용이며 이러한 내용이 공개되거나 불순한 이용자에게 들어가면 큰 해를 끼칠 수 있게 된다. 또한, 이러한 파트너와의 연구는 중요한 투자로서 데이터의 손실이나 침해는 재정적 손실을 불러온다.

7.2. 사적 영역 프로그램 (PSP) 파트너 이행 절차

7.2.1. NCSA 직원 및 파트너

사적 영역 프로그램의 AD (PSP AD)는 파트너와 감독사무국 사이의 보안에 대한 책임을 가진다. 이는 파트너의 NCSA에 대한 요구 조건 및 관심 사항에 대하여 NCSA는 해당 사항에 대한 보안 및 절차를 고지해야 함을 의미한다. PSP AD는 비밀 보호 계약의 속성에 대하여 모든 NCSA 담당자에게 고지하여야 하며 양자간의 승인된 비밀 보호 문서의 blank-copy 파일을 만든다. 이와 같은 비밀 보호 문서에 서명한 PI의 모든 담당 직원은 이러한 계약서의 사본을 받게 된다.

7.2.2. 파트너 관계

PSP AD는 사적 영역 프로그램 (PSP) 파트너와 NCSA 사이의 상호 작용을 조율하는 책임을 가진다. 해당 직원은 보안에 관련된 의문 및 문제 발생시에 접촉할 수 있는 가장 중요한 대상이 된다. 이는 PSP AD의 접촉이 어려운 긴급한 상황에서 파트너의 다른 직원에 대한 접촉을 제한하지 않는 것을 포함한다. 이러한 관계의 조율에 대한 세부 내용은 아래와 같다.

- 파트너의 보안 부서 방문을 조율한다.
- 계약에 따른 보안 조항을 감시한다.

- NCSA/사적 영역 프로그램 (PSP) 보안 정책 및 절차에 대하여 이를 새로운 파트너에게 설명한다.

- 보안 정책 및 절차에 변동이 있을 경우 이를 파트너에게 고지하고 이에 따른 프로젝트에 대한 영향 및 민감한 정보의 취급을 설명한다.

- 모든 문제에 대한 조사를 지원한다.

7.2.3. 파트너 사무실

사적 영역 프로그램 (PSP) 파트너를 위한 사무실 공간은 공동의 사무실로 부여된다. PSP 파트너는 NCSA에서 특정 공간을 사무실로 배정 받을 수 있다. 또한 양자간의 법적 계약을 통하여 파트너가 활용할 수 있는 공간을 배정 받을 수 있다. 특정 파트너의 공간 확장에 대하여 담당 직원들은 이러한 파트너의 공간을 존중해야 한다.

a. 사람이나 재산, 또는 자연 재해 (홍수 등), 인재 (화재 등), 또는 의도적 범죄 (사무실 내에서의 불순한 사용 등)에 따른 비상 사태가 발생한 경우 NCSA 직원은 이러한 문제를 인지할 수 있는 메커니즘을 통하여 문제 해결을 목적으로 PSP 파트너의 사무실에 접근할 수 있다. 이러한 NCSA 직원의 비상 접근은 파트너 사무실 접근 규정에 따라 고지된다.

7.2.4. 특정 파트너 요구 조건

파트너의 개개인은 계약 조건에 따라 자신들의 사무실, 컴퓨터 장비, 제트워크 또는 사적 정보 등에 대하여 특별 보안 및 보호를 요청할 수 있다. 이러한 요청 및 이에 따르는 이행에 대한 감독사무국 및 PI에 대한 조율의 책임은 PSP AD에 있다.

7.2.5. 출판 및 발간

NCSA 및 이의 고용인들은 NCSA에서 이루어진 연구 결과에 대하여 출판 또는 발간 등에 대하여 아래의 조항에 따른 권리를 갖는다.

1. 완성된 결과물에 대한 복사 물의 출판 및 발간은 실행에 앞서서 적어도 30일 이전에 파트너에게 공지해야 한다.

2. 만일 파트너가 해당 자료에 사적인 정보가 포함되었음을 인지한 경우 파트너는 문서를 통하여 30일 이내에 대학 당국에 해당 사항을 알려야 한다. 이러한 보고에 대하여 대학은 해당 사적 정보를 출판 또는 발간 자료에서 삭제하여야 하거나 이를 취소하여야 한다. 새로이 갱신된 모든 자료는 파트너가 검토할 수 있도록 다시 제출되어야 한다. 파트너는 이러한 규정에 따라 권리를 주장할 수 있다. 만일 파트너가 이러한 30일의 기한 내에 이의를 제기하지 않을 경우 해당 자료는 자료의 저자에 의하여 출판 및 발간이 이루어질 수 있다.

3. 만일 파트너가 이러한 출판 및 발간을 위한 자료에 특허에 준하는 매우 중요한 자료가 있음을 인지한 경우 파트너는 해당 출판 및 발간 30일 이전에 대학 당국에 보고해야 한다. 이러한 보고에 대하여 대학 당국은 파트너의 자료를 합법적으로 보호하기 위하여 보고가 접수된 날짜로부터 3 개월의 유예 기간을 허용 (이러한 유예 기간은 대학 당국의 협의에 따라 사안에 따라 연장될 수 있다) 할 수 있다. 이에 따라 해당 자료의 저자는 자료의 공개를 피할 수 있는 수정의 기회를 가질 수 있게 된다. 모든 갱신된 자료는 파트너의 검토를 위하여 다시 고지되어야 하며 파트너는 규정에 따라 해당 자료에 대한 권리를 갖는다. 만일 파트너가 이러한 30일의 기한 내에 해당 출판 및 출간 자료에 대한 이의를 제기하지 않을 경우 해당 자료는 자료의 저자에 의하여 지연 없이 출판 및 발간이 이루어질 수 있다.

PSP 사무국은 파트너의 모든 요청에 대한 준비 및 제공에 대한 책임을 가진다. 핵심 저자는 해당 자료의 처리가 정상적으로 이루어지는지고 정상적인 파일로 이루어지는지에 대한 확인을 위하여 PSP 사무국에서 같이 일을 할 수 있다. 여기에서 핵심 저자가 해당 사항을 대학 당국에 고지를 하지 않은 경우는 공동 저자(들)이 이에 대한 책임을 가지게 이는 적절한 문서로 이루어진다.

PSP 사무국은 파트너 관련 연구의 출판 및 발간 책임에 대하여 규정에 따라 참여자에 공지한다.

7.2.6. 우발적 공개에 대한 보고

모든 직원은 파트너의 기밀 또는 사적 자료, 또는 파트너에 영향을 주는 보안 사고 (장비 사고)에 의한 우발적인 사고에 대하여 주의를 기울여야 하며 문제가 발생한 경우 즉각 보안 사무국 또는 PSP AD에 보고 하여야 한다. PSP AD는 OVCR (Office of the Vice Chancellor for Research)의 책임자, 그리고 파트너에

대한 공지의 책임을 지는 감독 사무국에 이를 고지하는 책임을 가지며, 이러한 고지 과정은 사안에 따라 즉각적으로 이루어져야 한다.

8. 부록

8.1. 세부 사항의 규정

PSP AD: 사적 영역 프로그램 (PSP)의 조감독

할당 시스템 (Allocated systems): 학술 연구원에 대한 컴퓨팅 자원의 할당이 이루어진 시스템. 시스템의 자원 사용을 위하여 사용자에게 각각의 계정이 주어진다. 이러한 시스템들은 보통 생산 컴퓨터 자원 또는 슈퍼 컴퓨팅 자원으로 불린다.

동료 참여자 (Collaborator): NCSA 프로젝트에 참여하는 연구원. 이러한 연구원은 사적 영역 파트너, 학술 파트너, 그리고 사업적 파트너를 포함한다. NCSA 고용인은 보안 목적을 위한 NCSA 동료 참여자라 할 수 있다.

계약 (Contractual Agreement): NCSA와 참여자 사이의 공식적인 계약을 의미한다. 이러한 계약의 보기로서 Operational Agreements 또는 Memorandum of Understanding 등을 꼽을 수 있다.

DD: 지국장 (Division Director). NCSA의 지국장들은 감독관에게 해당 지국의 직원들에 대한 모든 보고의 책임을 가진다.

DO: 감독 사무국 (Director's Office). DO는 사무국의 국장, 사무 국장, 과학 부장, 기술 부장, 그리고 여러 명의 지국장들로 구성된다.

수출 제한 (Export Controlled): 기술 자료 또는 문서 등 일부 자료는 영구적으로 미국 내 또는 다음의 국가에서만 사용될 수 있는 수출 제한을 가진다. 이들 국가는 Austria, Australia, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, 또는 the United Kingdom를 의미한다.

사고 대응 팀 (IRST, Incident Response and Security Team). NCSA IRST는 NCSA 보안 팀에 의하여 운영되며 이는 운영 직원, 네트워크 관리자, 그리고 시스템 관리자로 이루어진다.

기계실 (machine room) 이는 특정 장비를 위한 공간으로서 승인된 관리자 또는 직원에 의하여 관리된다. 대부분의 건물에 NCSA에 귀속된 기계실이 존재한다.

NCSA 제어 영역 (controlled area): NCSA 직원에 의하여 소유되고 관리되는 기계 또는 자원을 의미한다.

OVCR (Office of the Vice Chancellor for Research). 이 사무실은 수석 캠퍼스 감독관을 위한 것으로 University of Illinois at Urbana-Champaign에서의 첨단 연구에 대한 책임을 가진다.

PI (Principal Investigator). PI는 동료 참여자와 수행되는 프로젝트를 의미한다.

PCF (Petascale Computing Facility) Blue Waters 시스템이 설치된 시설을 의미한다.

생산 시스템 (Production system) 이는 NCSA의 중앙 관리에 의하여 관리되는 자원으로서 24x7x365의 규모를 가진다. 이 장비는 전자 메일 서버, 웹 서버, 파일 서버, 그리고 다른 중요 인프라 자원을 포함한다.

보안 영역 (Security action) 보안 영역은 원하는 수준의 보안을 제공하기 위하여 적용되는 일련의 절차를 의미한다.

보안 사고 (Security incident) 보안 사고는 문서화된 절차 또는 과정, 또는 민감한 정보 등에 대한 침해를 가하는 행위 또는 상황을 의미한다.

민감한 자료 (Sensitive materials) 이는 보호 (기밀, 사적 또는 수출 제한 대상 자료)가 필요한 대상을 의미한다.

직원 (Staff) 직원이라 함은 NCSA의 고용인 (보수 및 무보수의 정규직, 비정규직, 그리고 학생 직원)을 포괄하며 NCSA의 프로젝트에 종사하는 인력을 말한다.

사용자 (User) 사용자는 NCSA의 자원을 이용하기 위한 승인된 계정을 가진 모든 사람을 의미한다.

방문자 (visitor) 방문자는 NCSA 빌딩 및 사무실을 방문한 직원 이외의 모든 사람을 의미한다.

8.2. 대학 정책 기준 자료

University CIO Policy page:
http://www.cio.illinois.edu/policies/index.html

University Academic Staff Handbook
http://www.ahr.uiuc.edu/ahrhandbook/default.htm

Campus Policy and Procedure Manuals
http://www.fs.uiuc.edu/luci/

빈 칸

NCSA Security Policies and Procedures

Updated June 26, 2009

Table of Contents

1. INTRODUCTION

This document establishes NCSA security policy and procedures. It provides methods for security policy development and implementation, assigns responsible management, and establishes procedures for security implementation and review, and resolution of security conflicts or incidents.

NCSA's computing and intellectual environment includes academic, government, and private sector researchers. The sensitivity of information and the openness of exchange are different in each of these environments. However, the history of NCSA shows the value of facilitating intellectual exchange and collaboration within and between these communities. NCSA's security policies and technical security architectures are designed to provide mechanisms whereby researchers can implement the level of security appropriate for their work.

NCSA's security strategy is to provide staff with tools and education concerning security policy and procedures, relying on individuals to use this knowledge and these tools to implement security measures appropriate to their work. In addition, centralized security measures and controls are implemented to assure basic security and to provide administrative review of security.

NCSA supports a variety of computing systems, services, and research projects for a diverse set of national and international academic, government, and private sector users. It is the responsibility of each participating user, staff person, or organization to use the tools available at NCSA to protect its assets and those of its staff and collaborators from injury, theft, or unauthorized use. Primary security concerns for NCSA include:

- Personal security of staff while working at any NCSA site including protection of personal possessions kept on site.

- Physical security of buildings, equipment, and records including protection from fire, theft, and unauthorized use.

- Protection of sensitive materials (see Definition of Terms). This includes compliance with non-disclosure and other security related agreements. Typically vendors or research partners provide information that they do not want distributed to others or used for purposes other than those stated in the agreement.

- Protection of the advanced computing and information infrastructure including the management of the computing systems and networks to prevent unauthorized use or denial of services, and to provide the protection of intellectual property (text, software, and data) stored or processed by those systems.

1.1. MISSION STATEMENT

The NCSA Security Policy and corresponding security standards, guidelines or procedure documents have been developed to provide reliable protection of various NCSA assets. These assets may be resources (computational systems, printers and copiers), information (e.g., intellectual property), infrastructure (e.g., networks and facilities), or relationships (e.g., agreements with private sector partners). Considered threats to these assets include—but are not limited to—direct cyber attacks from outsiders, improper resource use by employees and users, accidental disclosure of sensitive data, and natural disaster.

The NCSA Security Team's role is to (1) educate users on how to properly handle sensitive information and use their computers in a security conscientious manner; and (2) to support the central mission of the center by assuring confidentiality, integrity, and availability of its resources to its staff and researchers. In close collaboration with other NCSA groups, the Security Team helps protect our resources by focusing on assessing, detecting, and mitigating the risks to our network and computational systems. This policy document establishes a baseline of policies, as well as, standards and procedures that apply to all NCSA employees in order to meet these goals. Furthermore, it is the responsibility of the Security Team to maintain this document, update it and assist users in complying with it.

This policy and any corresponding documents are intended to be distributed to all NCSA employees, including full-time, part-time and student employees. This policy document itself is not sensitive, and its public disclosure would pose no threat to NCSA assets.

1.2. POLICY SCOPE

The NCSA Director's Office (DO) is ultimately responsible for establishing and implementing security. Any member of the Director's Office or any NCSA Division Director (DD) may be consulted concerning security policy and procedures for their respective division. Each DD is responsible for ensuring that the security policy and procedures are followed in their division.

This policy has been approved by the Director's Office and applies to all NCSA employees both current and future. This includes full-time, part-time, student and hourly employees. It does not include the vast user base of the NCSA's HPC resources, who fall under a separate user agreement. It applies to the use of any NCSA equipment and facilities, and personal equipment if attached to NCSA networks or storing NCSA intellectual property.

This policy does not replace the University of Illinois security policy, but is held in addition to it. NCSA is a department within the University of Illinois, and is thusly bound by all policies and procedures of the University. If there are any discrepancies between the University's policies and NCSA's, then the University's takes precedence. However, where it is more restrictive, this policy takes precedence. Likewise, this policy does not necessarily address criminal or civil laws regarding the handling of special data (e.g., medical records) which may be more restrictive.

Furthermore, particular projects and partnerships at the NCSA may have additional security requirements. For example, the Blue Waters petascale computing project with IBM has additional confidentiality requirements derived from contractual agreements, and as such it has an additional security policy. Therefore, employees on that project may have additional rules to follow where that policy is more restrictive than the general NCSA policy.

While some computer systems require additional physical security protection mechanisms, this document is primarily aimed at information and cyber security. The NCSA Security Team is responsible for information and cyber security, and building security falls under the jurisdiction of the Administrative Office.

1.3. RELATED POLICIES

The University of Illinois Information Technology Policies[1] address some additional topics not covered in this NCSA policy and some of the same topics to greater detail. These policies also apply to NCSA employees as NCSA is a unit of the University. These topics include, but are not limited to:

- Software piracy, file-sharing and peer-2-peer utilities;
- Bandwidth usage;
- Handling of Personal Identifying Information; and
- Privacy policy and rights of individuals.

2. AWARENESS

It is the policy of NCSA to provide an appropriate level of personal, physical and information security. Staff and others working at NCSA are required to read this document and take steps as needed to assure security. When security related questions arise they should be directed to one's supervisor, DD or the NCSA Security Officer.

Each staff member shall be provided with a copy of this NCSA Security Policy and Procedures document upon arrival to NCSA during the HR orientation process. It should be reviewed with his or her supervisor or DD during the first week of employment. The general policies and procedures as well as the detailed procedures for the person's particular division and work should be reviewed. The briefing should cover all the sections of this document. The new employee must acknowledge that they have read and understand the security policy, and this will be documented with a security acknowledgement form to be signed by the employee. A paper original form may be kept in the employee's folder in Human Resources (HR), otherwise an electronic acknowledgement by the employee will be stored in a database accessible by HR and the Security Team.

All new staff members are required to attend the first available new employee security training session. These sessions are held regularly, though a regular session may be postponed if there are only a few eligible attendees. Information on dates and times of sessions can be obtained from HR or the NCSA's Security Officer.

Each division should engage in a review of security policies and procedures pertaining to that division's activities at least once a year. Divisions will routinely monitor system and administrative activity related to security and the overall compliance of NCSA staff with security policies and procedures. Care will be taken to perform these reviews in an environment and manner that promotes contributions from the staff and makes them part of the effort of defining the procedures and proper levels of security. The DD will insure that these reviews are completed, and generate recommendations if needed.

Proprietary information will be clearly labeled (see section 6.4). Such outward, visible signs are useful in emphasizing to staff the importance of security in general. Staff are required to make use of this mechanism to maintain a sufficient level of awareness of security issues.

Supervisors will consider security procedure compliance when completing staff performance evaluations.

Security issues will be addressed with departing staff during exit interviews performed by HR (see section 6.3).

3. ASSURANCE

Defining and implementing appropriate security levels requires a continual process of confirming that both the defined policies and procedures are adequate for the ongoing work of the center, and that those policies and procedures are being properly communicated to and carried out by the staff and users. NCSA provides such assurances through a number of organizational and operational facets.

3.1. NCSA SECURITY TEAM

The NCSA computational security team, referred to just as the Security Team, helps to set guidelines and insure the integrity of the NCSA computer and network environment. They actively track and respond to security vulnerabilities and incidents. The Security Team also includes the Incident Response and Security Team, IRST (see Definitions of Terms).

3.2. STAFF RESPONSIBILITY

Each working area will have a DD as well as an individual staff member or members responsible for carrying out certain details of the policies and procedures for that area. It is the DD's responsibility to see that the detailed procedures section is maintained and followed in the daily activities of the staff in that area. The DD shall respond to requests for information from staff on specific procedures and interpretation of security policies.

It is the responsibility of each staff member to follow the procedures defined for an area in which he or she is engaged. It is also their responsibility to understand the underlying policies that drive those detailed procedures, so that the individual is able to make rational decisions in certain situations not specifically covered by the detailed procedures. However, in the latter case, a further responsibility exists to report the situation (described below) and have procedures clarified for future reference by other staff. Each staff member is expected to report any known or suspected violations of security procedures, or any exposure of known sensitive material to unauthorized personnel. This report should be made immediately to the NCSA IRST Team as identified in section 6.2 of this document.

Failure to comply with the policies and procedures within this document can result in disciplinary actions, up to and including termination, as per University and NCSA policy (see section 8.2).

4. NCSA FACILITIES PHYSICAL SECURITY

4.1. PHYSICAL SECURITY

This section of the NCSA security policy is concerned with physical security. All references to security in this section are related to physical security. Issues of electronic data security and intellectual property are covered elsewhere within this document. Physical security includes building and room security as well as physical security devices such as locks and physical restraints. Physical security is related to electronic data and intellectual property security. The ability to physically access a computer or paper files may compromise the security of electronic data. Physical security depends on many things. Building construction details such as the type of floors, walls, roof and especially windows are important. Windows that can be opened more than six inches are a security risk, especially at ground level.

Alarms and other security systems tend to increase building security. Some of the types of security systems in NCSA buildings are door monitor systems and after-hours motion detection and alarm systems.

The type, quantity and value of equipment and information located in NCSA buildings are important security factors. The more desirable or marketable these items are, the more likely it is that someone will attempt to breach NCSA security.

4.2. NCSA BUILDING SECURITY

As of September 2005, NCSA is located in two campus buildings (Advanced Computations Building, and NCSA Building) on the University of Illinois campus. The Petascale Computing Facility is under construction in 2009, which will eventually replace the Advanced Computations Building for our needs. The nature of these buildings directly affects NCSA physical security. Following are descriptions of the security systems, procedures and related issues for each building. Plans of all NCSA space indicating room usage and occupants are maintained and are available at request from the Director for Administration.

NCSA's normal business hours are from 8:00 a.m. – 5:00 p.m., Monday through Friday, except holidays. In general, visitors are not required to sign-in. All University buildings are cleaned by Building Service Workers (BSW) and maintained by trades people employed by Facilities and Services (F&S). All University buildings have space allocated to F&S for BSW's and mechanical systems.

4.2.1. Advanced Computations Building (ACB)

NCSA occupies all of ACB with the exception of space dedicated to mechanical systems and custodians. ACB entrances and computer rooms are to be locked at all times and use a keycard system to gain entry. Video cameras are located at all entrances and are monitored by staff in the control room. An intercom and remote lock release system is used at the main entrance to allow entry to authorized personnel who do not have keycard access. ACB is not open to the general public and is staffed 24/7/365.

4.2.2. NCSA Building

The NCSA Building is where most of the NCSA staff are located. North and south doors are open during regular work hours, and require key card access after hours. Side doors are locked and require key card access at all times. The NCSA Building also has surveillance cameras at all entrances.

4.3. PHYSICAL SECURITY REQUIREMENTS

All building exterior doors are to be kept locked at all times except where specific procedures have been established to leave a door unlocked. Doors shall be left unlocked or open only while a staff member is in a position to monitor access through the doorway. No one shall provide or allow unescorted access to any building or room to anyone who is not known to them to be a trusted staff member. Staff are encouraged to challenge in a non-offensive manner anyone in an NCSA building or room whom they do not know. Any person who is suspicious or cannot provide staff identification must be reported to either your supervisor, DD, or the University police. If you witness a building problem, such as a faulty lock or door, a propped open door, or something potentially dangerous, you must notify your building maintenance department, supervisor, or DD.

Individual workstations are subject to the physical security of the users' offices. Users must control physical access to their office and thus their computer. All rooms shall be kept locked unless a staff member is in the room or within sight of the room (in a position to monitor access to the room) or specific procedures have been established to allow the room to be left unlocked. Staff may choose not to lock a room for brief periods during regular working hours if the room does not contain sensitive materials (see below). However, staff are advised to lock all rooms any time no one is there to monitor access (if for no reason other than protecting personal items).

All computer rooms and telecommunications closets/rooms are to be kept closed and locked. Allocated systems, production servers (see Definition of Terms) and related equipment are located in designated computer rooms. These rooms are to be locked with controlled access.

Laboratories and training rooms containing concentrations of computers and other valuable and/or sensitive equipment are to be kept locked with access limited only to authorized staff. In cases where public access to NCSA computers is allowed, security is maintained with physical locks and logon restrictions.

Confidential and proprietary information may be kept and used in various offices and other rooms throughout NCSA. Because it is not possible to control who may access NCSA spaces during regular business hours, and even after hours, NCSA staff are advised to lock their offices whenever they are away.

Office and building keys are distributed to NCSA staff and affiliates based on the Keys and Keycards policy (see Key and Keycards policy). Keys are requested via a form by supervisors and approved by the DD. Master keys are generally given only to senior full time staff and require the approval of the Director for Administration. The security team will coordinate with the DD of Facilities to perform regular audits of personnel who are listed as having master keys.

Equipment in an employee's office is the responsibility of that employee. If any equipment is moved, broken, replaced, or upgraded the Shipping and Receiving department must be notified.

Staff who use NCSA equipment off-site are responsible for the physical security of that equipment. Any NCSA equipment taken off-site needs approval by a supervisor and an Off-Site Equipment Usage Authorization form needs to be filled out with

Shipping and Receiving. This equipment is tracked through inventory control and audited annually by the Shipping and Receiving department.

If your NCSA-issued equipment becomes lost, immediately report this to inventory control via Email (shiprec@ncsa.uiuc.edu).

If your NCSA-issued equipment is stolen then a police report will need to be filled out. You can contact the University Police by calling 333-1216. If the item is valued over $300 then you will need to call 333-8911. An officer will need to come and take a report in person. Once the police report is filed, a copy will need to be sent to Shipping and Receiving so that it can be removed from inventory.

If your NCSA-issued equipment becomes damaged and needs repair, contact your supervisor.

Machines that are decommissioned (surplused/scrapped) are to be sent to the Shipping and Receiving department. Prior to these machines being decommissioned the hard drives will be wiped so that data is unrecoverable in accordance with the Illinois Data Security on State Computers Act. The procedures for wiping the disks will follow the Illinois Public Act 093-0306 and industry best practices.

Machines that are swapped internally between individuals or groups, which contain proprietary data (original or derived), will need to have the hard drive wiped. The same procedure as above will be utilized on these machines.

5. NETWORK AND SYSTEM SECURITY

Network security deals with concerns about the integrity and confidentiality of data traversing the network as well as the potential for security incidents (denial of service, unauthorized access, etc.) that occur over the network.

5.1. INTERNET ACCESS TO NCSA

NCSA's Internet connections provide high performance access to NCSA resources. Internet access is provided through a set of Internet routers which may be configured with a number of packet filters and other "firewall" mechanisms in order to prevent certain types of attacks from entering NCSA or originating from within NCSA. Detail on NCSA's filtering or firewall mechanisms are available from NCSA's networking group or security team.

5.2. NCSA INTERNAL NETWORK

NCSA operates a backbone network between its multiple buildings. All connections to the backbone network will have termination points within NCSA-secured network closets in each building.

With the exception of networking (routers, switches, etc.) and security equipment (monitors), no computing devices are to be directly connected to the backbone.

Only NCSA or University owned equipment, or equipment that is approved by a users direct supervisor, is allowed to be connected to the NCSA network. This includes personal laptops, PDAs and wireless access points.

Wireless access to NCSA's internal network is through NCSA's managed wireless access points. No other access points are allowed to be connected to the NCSA network without approval of an individual's supervisor or DD, and coordination with the supervisor of Network Engineering.

5.3. COMPUTER SYSTEM SECURITY

There are two types of computing security on which NCSA has focused. These are 1) operating system security and 2) user data security. While these two types may be seen as having distinct boundaries between the users' and NCSA staff's responsibilities, both NCSA and its user communities must work together to ensure a secure environment for all.

The operating system security goals are fivefold: to prevent access to the systems by unauthorized users, to prevent users with valid logins from unauthorized data access, to prevent unauthorized use of computing resources, to maintain system availability, and to prevent errors by those authorized to make system level changes.

The security for the operating system environment is shared by the system administration staff of NCSA for those systems that are centrally managed, NCSA staff and researchers who choose to manage their own systems, and the vendors of NCSA operating systems.

Administrators of all machines are required to keep their machines up to date with the most current patches to the operating systems. All unnecessary services should be

disabled. System scans may be performed by the security team for vulnerabilities on all NCSA machines, and administrators may be notified to install specific patches to address vulnerabilities (see section 5.8).

Machines running production services (e.g. web, email, database, etc.) are required to be located in a machine room (see Definition of Terms).

Administrators running Windows machines are required to install and run the NCSA site licensed anti-virus package, or another licensed anti-virus package approved by the NCSA security team. These also need to be kept updated according to the vendor's recommendations.

Individuals may choose to maintain and provide the management of their own systems subject to the approval of their supervisor, but they accept full responsibility for the security of that system and any systems that may be compromised due to negligent security administration of that system. For student machines, it is the responsibility of their immediate supervisor to ensure they are maintained in a secure manner. Administrators of systems must also make themselves available to the NCSA security team at any time for security related incidents that involve systems they administer.

If a machine appears to have been compromised it may be taken off the network by the authority of the NCSA security team.

If you feel your electronic workplace (e.g. your account, or machine you manage) is compromised, or if you observe suspicious electronic behavior you are not sure about, immediately cease access to the system (but do not turn off the system) and contact NCSA Security. NCSA Security can be reached via the NCSA Help Desk (217) 244-0710 or <help@ncsa.uiuc.edu>.

The security of NCSA computing systems has been designed to enhance the collaborative effort of those scientists who choose to work in the NCSA intellectual environment. NCSA policy is that the user should make the decisions regarding data sharing and has provided tools and instruction to its users to enable them to do so. Users are encouraged to make every effort to secure their own data.

5.4. ACCOUNT SECURITY

All accounts on NCSA resources will be authorized by the NCSA allocation process before activation. For account management on self-managed systems, if a user has an account on an NCSA public resource then they are approved to be added to the local system. It is, however, the administrator's responsibility to make sure all accounts on the system(s) they manage are currently authorized by NCSA.

Accounts are for use by only the authorized individual and are not to be shared. Passwords and private keys should never be shared with anyone (this includes supervisors, coworkers, and spouses).

Users should maintain the secrecy of private keys associated with their accounts. Private keys may be used with programs like SSH, or PKI certificates. Long-lived private keys, need to be protected by secure passwords and stored in files readable only by the owner. Users should always enter secure passwords when prompted for a password to protect a long-lived private key and should not use blank or empty passwords. NCSA allows for passwordless short-lived private keys typically defined as lasting a week or less. If you suspect the secrecy of a private key associated with an NCSA account may have been compromised, contact NCSA's Security Team immediately as identified in section 6.2 of this document.

New user account information, along with default passwords, will be mailed to users and this document should be saved and secured for later reference. Instructions for users who have forgotten their password are contained in that document. Users should set a new password during the initial login. If a new password has not been chosen within thirty days of account creation, the account will be locked

Users of self-managed systems also need to follow the above procedures.

NCSA security staff may audit password files in an attempt to detect insecure passwords.

Accounts on allocated systems are centrally managed through the Allocations process. This process also regularly verifies valid accounts and can report any discrepancies.

System administrator accounts are maintained with strict permissions. Access to these accounts are centrally managed and monitored frequently.

NCSA does not allow clear-text passwords (static passwords over an unencrypted channel) for remote access to any systems. Kerberos, SSH, or other secure methods must be used.

Staff accounts are no longer authorized upon departure of the employee. Mass storage (mss) access is available for four months after accounts are deactivated. These access times are enforced on all allocated and production systems unless requests are made to your supervisor and approved by the DO.

5.5. FILE SYSTEM SECURITY

All system files on allocated and production machines are protected from user modification and are checked on a regular basis for modifications. Privileged programs are monitored as well for use or for unauthorized changes.

Remotely accessible file systems (such as NFS and Windows sharing) may be exported only to systems located on NCSA managed networks, and systems are not allowed to mount file systems from machines outside NCSA managed networks. Exceptions to this must be approved by the NCSA Security Team which can be contacted via *security@ncsa.uiuc.edu*.

In the course of their duties, system or security administrators may need to access files or directories in order to fix problems. But this is not to be done any more than is needed to correct the problem.

5.6. DATA CLASSIFICATION

There are three categories of data classification that require different levels of security. The three classes are:

- **Non-sensitive (Public)** — Information that may be freely disseminated.
- **Confidential** — Data that the owner feels should be protected to prevent unauthorized disclosure, but wouldn't expose NCSA to loss if disclosed.
- **Proprietary or Export Controlled (High Risk)** — Information assets for which there are legal requirements for preventing disclosure or financial penalties for

disclosure. Data which is covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, EAR 99, ITAR, and certain client specified data, which may include: contracts, non-disclosure forms, software, documents, and graphics. Such materials may also include intangible assets such as concepts, text, derived data, and graphic information in any form. Payroll, personnel, and financial information are also in this class because of privacy requirements.

These classes are coordinated with the University's Data Classification Policy section of the Information Security Policy, though they use the alternate labels in parentheses (e.g., *Public* and *High Risk*):

http://www.fs.uiuc.edu/cam/cam/viii/viii-1.2.html

The handling procedures for these are addressed throughout this document.

5.7. DATA INTEGRITY (BACKUPS)

Backups are performed periodically on all production and many desktop and laptop systems. These backups are done to ensure data integrity in the event of hardware failures. General scratch and temporary areas on the disks are not backed up since these data areas are very large and are considered as temporary storage space only. Duplicate backup tapes are stored in an alternate secure area at another NCSA facility. Backups are kept for 90 days and after that time the tapes may be recycled.

5.8. SYSTEM ADMINISTRATION SECURITY MONITORING

Computer systems security is a very complex issue. While certain tasks can be automated, the basic level of security must come from those administrators who, as part of their training and job responsibilities understand their respective systems. The number of administrators and the time spent on system security varies with each machine. When potential security problems arise the security team's approach is to gather as much data as possible regarding the security problem without compromising system or data security.

There are automated procedures that monitor log files and they may, at times, need to be monitored manually as well.

Security scans are done periodically on systems by the NCSA Security Team. These scans are done to assess vulnerabilities and other system exposures. Administrators will be notified of any problems, and recommendations of best security practices may be included. These scans will be kept for at least 6 months. The Security Team (*security@ncsa.uiuc.edu*) can be notified if there are any questions about the systems from which these scans are originating.

Host and network intrusion detection systems may be used by the security team to monitor and track intrusion attempts and compromises. In the event of an intrusion the security team may add additional monitoring for the period of time the system(s) are under investigation.

5.9. ELECTRONIC MAIL

As a productivity tool, NCSA encourages the use of electronic mail (email). However, users access the Internet, including email, at their own risk. NCSA is not responsible for anything received, downloaded, or viewed by users via the Internet. Specifically,

email may deliver unsolicited messages that contain offensive content or malicious software (computer viruses, worms, etc.).

NCSA cannot guarantee email will be private. Email can, depending on the technology, be forwarded, intercepted, printed, and stored by others. People other than the intended recipient may possibly access email. Email may be stored in backups in systems that may be retrievable after traditional paper letters would have been discarded or destroyed. Staff should be aware email is analogous to sending a postcard such that the content is not protected.

Users are prohibited from (1) having their NCSA email accessed (e.g., POP'ed) from another email service, and (2) forwarding their NCSA email to another service other than CITES Express Mail. Having other email services like Gmail access your NCSA account via POP or any other protocol is inherently insecure as it requires a third party to store your NCSA Kerberos password, and such password sharing is prohibited elsewhere in this policy for several reasons. While it may be convenient to forward your NCSA email to another provider such as Blackberry or Gmail, this results in a loss of control for the NCSA. For example, if a sensitive email containing proprietary information is accidentally sent unencrypted, we can no longer track or delete all copies of it. Furthermore, we have no control over the security mechanisms or privacy guarantees of third party email providers.

In the course of their duties, email administrators may need to look through users mailboxes in order to fix problems. But this is not to be done any more than is needed to correct the problem.

Email is scanned as it passes through the NCSA mail server for viruses, spam, or malicious software. Spam can be automatically tagged or blocked with this system if a user requests it. Requests for either of these can be directed to help@ncsa.uiuc.edu.

It is against NCSA policy for NCSA staff to email sensitive material (see Definition of Terms) without permission from the project lead or the owner of the sensitive information. However, the owner of the information may choose to email sensitive information at their own risk. Encryption techniques are encouraged for emails of a sensitive nature.

It is prohibited to knowingly pass along viruses, chain letters, hoaxes, or other unsolicited email.

5.10. INTERNET USE

Attempting to break into any computer system at anytime from any NCSA resource (e.g., computer or network) is strictly prohibited. Furthermore, releasing any worms or other malicious code on our internal network, or out on the Internet, is prohibited. The only exceptions are for situations approved by the NCSA Security Team (e.g., penetration testing), or research projects that are approved by a DD (e.g., approved security research projects with appropriate safeguards). Attempting to subvert or avoid any NCSA electronic security system, or to bypass any network-based security mechanism is similarly prohibited.

Intentionally obtaining, sharing, storing, viewing, emailing, or downloading items of an obscene or graphic nature including but not limited to, pornographic, sexist, racist, or illegal materials and/or any information/graphics that violate any of the policies of NCSA or the University is prohibited.

Using NCSA resources to advertise or sell commercial products and/or services is strictly prohibited. NCSA resources shall not be used for hosting Internet domains unaffiliated with NCSA related projects. The NCSA DO reserves the right to remove **any** content being served from its web servers—at any time—that it deems in appropriate or not inline with its mission and goals as an institution.

6. PROCEDURES

6.1. ESTABLISHING POLICIES AND PROCEDURES

Each DD responsible for a given area, requiring additional security policy and procedure definitions not covered herein, will be responsible for establishing these applicable specific security policies and procedures. In cases involving multiple NCSA divisions, the responsible DD's will work together or specify a responsible person to establish the additional security policies and procedures.

DD's will participate in internal and external security reviews or audits in order to analyze, justify and revise current policies and procedures as they apply to their divisions. DD's will establish a reporting line, as necessary, within their division which ensures that security is maintained in accordance with NCSA policies and procedures.

The Director's Office will be responsible for coordinating changes to security policy and procedures. A yearly assessment of the current policy and procedures document should be done to see if any changes are required. Requests for changes will be reviewed by the appropriate DD, who will report the feasibility and costs of the proposed changes. All changes in NCSA security policies and procedures will be approved by the DO. New policies and procedures will, in general, be assembled as a document that may be reviewed by the DO, as well as by the staff responsible for carrying out the specific procedures. New policies and procedures may be made part of this document at the discretion of the DO. NCSA staff and Private Sector Partners will be notified when changes are made to this document.

6.2. INCIDENT REPORTS REQUIRED

It is the responsibility of any staff member aware of a security incident (see Definition of Terms), to report it immediately to the NCSA Incident Response and Security Team (IRST). The IRST is reachable 24 hours a day through the HelpDesk (*help@ncsa.uiuc.edu*), or by phone at (217) 244-0710. IRST will then investigate the incident, notify affected parties (if needed), and recommend corrective actions.

6.3. EXCEPTIONS PROCESS

Realizing that we cannot predict all special circumstances that may arise, there may be valid exceptions (both temporary and permanent) to this policy in the future that we do not want to address by changing the policy as a whole. The process for requesting an exception to this policy is the same as the process for requesting a change to this document (Section 6.1), and the exception must be approved by both the DO and the Security Officer. The Security Officer will maintain a list of all currently valid exceptions.

6.4. SECURITY IMPLEMENTATION PLAN

The DD shall discuss security policy and procedures with supervisors in the division. The DD shall specify the steps to be taken by each supervisor. The DD and supervisors will review policies and procedures and raise concerns and issues for change and improvement to be taken to the appropriate DO contact. All security violations and non-compliance situations will be reported to the DO and the Security Officer. The DO and Security Officer will work to rectify these situations.

The following are specific actions and responsibilities.

- The DD should discuss security on a regular basis at meetings with supervisors and staff.

- Division-specific guidelines will be drawn up covering physical security and computational security activities where appropriate to that division.

- Supervisors will keep their staff aware and informed of policies and procedures, and be responsible for security within their own area.

- Supervisors will make themselves available to discuss the NCSA Security Policy and Procedures document with each new employee. Employees are required to read this document and address any questions pertaining to it with their supervisor. Supervisors should review with each new employee the security policies and address security issues specific their role and responsibilities. This procedure is to be documented through the use of an electronic security document acknowledgment form that will be electronically signed by the employee and then made available to HR.

- For staff working under non-disclosure agreements (NDA) the supervisor will work to help clarify the nature and purpose of these agreements. No one will be allowed to work on a collaborator project which requires a NDA unless a signed security document acknowledgement form, and a project-specific NDA, is on file with HR.

- HR staff will conduct an exit interview with a departing staff member prior to the staff member's final working day at NCSA. This interview will cover, among other things, keys and keycards that may need to be collected, and a review of the non-disclosure agreements in effect for that person (if any have been signed). A discussion of the personal effects of the staff member will be made to attempt to identify any proprietary materials that may be among them and guard against such material leaving NCSA with the person. An employee exit form will be filled out and filed with the HR department.

- Security training sessions for staff will be conducted on a regular basis.

- Staff members will make visitors aware of NCSA's security policy and procedures where appropriate. Visitors passes, keys or keycards that are distributed to visitors, will be collected upon their exit.

6.5. PROJECT SECURITY PROCEDURES

This section describes the procedures and policies to be followed on projects involving proprietary or other sensitive data. The most common type of project of this nature is one with a Private Sector Partner involving proprietary information, but any collaboration may need this degree of protection and it is therefore available to any researcher. Herein the researcher, whether a Private Sector Partner or not, will be referred to as the "collaborator".

Projects are activities in which NCSA staff works with collaborators to develop and deliver materials. Projects may involve planning, data transfer, processing or archiving, software development, hardware development, and reporting, including documentation and audio/visual materials. The project may involve people from various divisions within NCSA or the University. The DD responsible for the project has overall coordination responsibility for the project. For projects involving a Private Sector Partner, a primary point of contact at the DD level will be responsible for

tracking the project and in particular for overseeing issues related to proprietary information.

6.5.1. Planning

In cases where proprietary information may be discussed it shall be the responsibility of the collaborator to clearly identify all material that is considered proprietary. This should be documented in the contractual agreement (CA) (see Definition of Terms) between NCSA and the collaborator.

Any projects requiring NDA's will require a CA with the collaborator so that the NDA's can be tracked. The CA will list any personnel working on the project who are required to sign an NDA. A copy of the CA will, at minimum, be kept with the Principal Investigator (PI) of the project and the NCSA Security Officer. Copies of the NDA's will, at minimum, be kept with the PI of the project.

The NCSA PI for the project will be responsible to ensure that all NCSA personnel involved have signed appropriate security related forms (i.e. NDA's) and are aware of the security issues involved in the project. The PI will also make available upon request copies of any CA employees are working under, or any NDA an employee has signed.

No NCSA user should access proprietary information without signing the appropriate NDA and being listed on the CA with the owners of that data.

Security actions for planning include determining what security issues are for the project, and then proceeding with the following steps.

6. The project will be given a code name and/or number if requested by the collaborator. This code will be used throughout the project in internal and external communications and planning tools and documents to identify and track activities associated with it. No NCSA planning or archive documentation will include a textual name associated with the project that might reflect the specific or general field of study.

7. Project participants shall be listed in the CA. This validation list includes NCSA, collaborator, and any other personnel. It is to include all individuals who will be allowed access to proprietary project materials. It may only be amended by signed common agreement between the collaborator and the NCSA primary point of contact. The validation list must be amended if, during the project, people join or leave the project. Only persons included on the validation list may access sensitive materials in any form. All references to access limitations imply limiting access to those on the validation list.

8. Obtain from the collaborator a written statement which describes the security related aspects of the project and indicates what action are necessary to preserve security. Obtain non-disclosure or other security related forms to be signed and all project related materials that are considered proprietary. This statement should be included in the CA.

9. No work on a project will commence prior to obtaining signed CA's and any related documents (i.e., NDA's).

10. The PI and collaborator will address security issues included in the CA with the NCSA Security Officer.

6.5.2. Project Implementation

This involves access to collaborator concepts, documents, data (including software), and any hardware or other physical assets. Data may be analyzed and manipulated by a variety of software and hardware tools to create intermediate work and deliverable materials. Security issues may involve access to documents and data, as well as exposure to concepts/information. Visual display of data may involve computer monitor displays, and various media.

Requirements for initial data receipt, if any, will be documented in the NCSA Data Receipt Form. This form will specify the nature of the data (proprietary, confidential, etc.), how data is received, and any storage requirements.

NCSA procedures for data management and access begins when the data is transferred from a collaborator controlled area to an NCSA controlled area (see Definition of Terms). NCSA will follow procedures herein for data stored only on computer systems operated by NCSA. All computer directories, files, and temporary storage areas used to store proprietary materials during the project will be maintained so that access is limited to only those with authorization.

If proprietary data is received in physical form (e.g. CD's, tapes, etc.) it shall be labeled "PROPRIETARY" on the media itself (if not so already labeled). Electronic data will be labeled according to the requirements determined with the collaborator. Other labels are acceptable on a per project basis. For example, IBM prefers it use the term "IBM Confidential" for proprietary materials.

Periodic audits will be done on any projects that have proprietary data stored on NCSA resources. These audits will include reviewing the CA and all personnel who are requiring NDA's, personal access to data, and any other security requirements.

Collaborator data and research information must be protected during display and media recordings. All display and recording of proprietary material on film, video or other graphic media will be conducted in a manner so as to limit access.

All derived data is required to be handled as the original data received.

An amendment to the CA will need to be made, and signed, when work is going to extend past the CA's original deadline.

When the project is complete, the authorized collaborator representative will be responsible for the removal of sensitive material. NCSA will not retain any proprietary materials once the project is complete. If any proprietary material is discovered after the end of the project, it will be returned to the collaborator or destroyed. A NCSA Data Release Form will be filled out on conclusion of a project along with completing any exit forms for the project. The data release form will specify the methods of removal, or destruction, of data. Destruction of data will follow the industry best practices.

General system backups are performed to insure the integrity of the system and its data. Backups of sensitive project information may exist beyond the life of the project (see section 5.7).

6.6. PUBLICATION AND PRESENTATION

Publications and presentations are restricted to the obligations contained within the CA. There are specific publication and presentation policies addressed with PSP collaborators in section 7.2.5.

6.7. COPYRIGHTS AND RELEASES

As a general guideline, other than periodic review of potentially proprietary materials and securing clearances, the NCSA staff will take no special security measures unless requested. It is up to the owner of information to request special measures and to specify appropriate restrictions on the dissemination of sensitive information. When such a request is made, it must be done in writing and appropriate signatures affixed.

Copyright will be confirmed with collaborators providing text or graphic materials before such materials are included in any NCSA releases of printed or electronic material. If necessary (i.e., if such materials are not owned by NCSA or do not reside within the public domain), written permission to reproduce any such materials will be secured from the copyright holder prior to any NCSA use.

Also refer to the "Copyright Policies and Issues" page from the University:

http://www.cio.illinois.edu/policies/copyright/index.html

6.8. NEWSLETTERS AND PUBLIC INFORMATION AND TECHNICAL MATERIALS

Staff will verify that written material submitted for inclusion in newsletters and other materials is not proprietary by following the same procedures above. It is the responsibility of the collaborator to specify in writing to NCSA, or otherwise note during the pre-publication review process of the material, if proprietary information is mistakenly submitted for an article, press release, or other publication.

Staff will also follow these procedures:

- Illustrative material obtained from internal NCSA sources: Verification with NCSA staff will need to be done to resolve copyright issues before such material is included in publications.

- Background or illustrative material not owned by NCSA: The staff will confirm copyright information with the contributor before inclusion in any publication. The contributor will be required to sign a standard release form. If any materials are to be restricted from dissemination, the contributor will specify it on the release form. A copy of the form showing restrictions will be provided to all staff involved.

- Permission to copy: staff will ensure that we have permission to duplicate vendor documents.

6.9. EMPLOYEE EXIT PROCESS

Several steps must be taken when an employee leaves to protect the security and intellectual property of the NCSA. Many of these steps will be done automatically when the manager fills out the **mandatory** exit form, an important procedure for all departing employees—full-time, part-time and student workers. These procedures are described below.

- All inventoried equipment must be transferred to other employees or surplused through Shipping & Receiving on or before their last day of employment. If the device has proprietary or confidential information on it, it must be wiped before being transferred to another employee. Shipping & Receiving must wipe **all** data before surplusing devices.

- Allocations will deactivate accounts—including the Kerberos principle—for the departing employee as soon as possible. However, the employee's files that are stored in a shared file system may reside in backups for up to 1 year. This would include files in AFS, MSS or messages on the email server.

    - The departing employee may still have some affiliation with the NCSA and need an account for research partnerships or other activities. In this case, they can get a sponsored guest account before they leave. However, the account name must be different. This forces system administrators to actively grant them access to any non public servers. Not changing the account name could inadvertently leave the former employee with access to several internal machines. This is a consequence of the decentralized manner in which servers and services are administered at the NCSA. This procedure would result in the email account for the old account being deactivated.

- Email accounts must be deactivated immediately following termination. Deactivating an email account means the user will no longer be able to login to NCSA's mail servers to check their email. However, while the former employee can no longer access the email system, the email administrator may provide an alias from their old NCSA address to a new email address upon request. In this manner, mail sent to the user's NCSA email address would be delivered to a non-NCSA account.

    - It is very important that a departing employee is promptly removed from any NCSA email lists. Exceptions can be requested by a manager on a per person per list basis. Furthermore, any lists administered by the former employee must either be terminated or transferred to another employee's control.

- Physical keys must be returned and key card access disabled on or before the last day of employment.

7. PRIVATE SECTOR PARTNER PROGRAM

7.1. PRIVATE SECTOR PROGRAM (PSP) PARTNER CONSIDERATIONS

The Private Sector Program Partners (PSP partners, or just partners) have specific security requirements due to the nature of their work and our interaction with them. Much of the research conducted with our partners is highly sensitive and could cause significant harm to the corporation's competitive position if it were to fall into the wrong hands. Additionally, much of the work done here with our partners represents a major investment, and loss of the data or alteration of the data could cause a financial loss. Any dealings with partners should reflect sensitivity to the security of their data.

7.2. PRIVATE SECTOR PROGRAM PARTNER PROCEDURES

7.2.1. Representation with NCSA Staff and with Partners

It is the responsibility of the AD of the Private Sector Program (PSP AD) to act as a liaison between the partners and the DO in regard to security matters. This includes representing partner needs and concerns to NCSA and representing NCSA policies and procedures to the partners. The PSP AD will work with all NCSA staff to clarify the nature and purpose of non-disclosure agreements with the corporations and maintain a file of blank copies of the approved nondisclosure document for each company. PI's of any staff signing non-disclosure agreements will receive copies of the agreements.

7.2.2. Partner Interactions

The PSP AD is responsible for coordinating interactions between the Private Sector Program Partners and NCSA. He/She is the principal point of contact for the partners when a security question or issue arises. This does not restrict partner access to other staff, particularly when timeliness is important and the PSP AD is unavailable. Coordination includes, but is not limited to, the following:

- Coordinate visits by partner security departments.
- Oversight of security provisions in any agreements.
- Briefing new partner on-site representative on specific NCSA/Private Sector Partner Program security policies and procedures.
- Notifying partners if changes in the security policy and procedures document impact partner projects or the handling of sensitive materials.
- Support investigations of any incidents.

7.2.3. Partner Office Space

There is a shared office space for Private Sector Program Partner use. On occasion PSP Partners may be assigned a designated office space at NCSA. The legal agreement with each of those partners clearly establishes that the partner controls access to their assigned office. Each member of the staff must respect the office as if it were an extension of the particular corporation's headquarters.

b. In the case of an emergency where there is immediate danger to people, property, and/or legal liability which may be the result of a natural disaster (e.g. flood), man-made (e.g. accidental fire), or illegal/malicious computer activity (e.g. a machine within the office space performing illegal/malicious activities), a mechanism will be established for NCSA staff to have emergency access to PSP Partner office space for the sole purpose of addressing the danger. This emergency access mechanism for NCSA staff will include attempting to reach designated Partner contacts for notification.

7.2.4. Specific Partner Requirements

Individual partners may request, through contract negotiations, special security safeguards for their office space, computational equipment, networks and/or proprietary information. It is the responsibility of the PSP AD to communicate any such requests and final agreement to the DO and the PI's involved in the process.

7.2.5. Publication and Presentation

NCSA and its employees have the right to publish or otherwise disclose the results of the research performed at NCSA, subject to the following conditions:

4. A copy of the proposed complete manuscript for publication or presentation materials for other public disclosure must be submitted to the Partner at least thirty (30) days prior to any submission for publication or public disclosure.

5. If the Partner determines that their proprietary information is disclosed in any manuscript or presentation materials, the Partner is required to notify the University in writing within thirty (30) days of its receipt. Upon notification, the University will have proprietary information deleted from the paper or presentation or have the publication canceled. Any revised manuscript or presentation materials must be resubmitted to the Partner for review. The Partner has the right to object on the basis of criteria specified above. If the Partner fails to respond within thirty (30) days after its receipt of the initial manuscript or presentation material or subsequent revision, the author(s) may proceed with publication or public disclosure.

6. If the Partner determines that potentially patentable subject matter is contained in any manuscript or presentation materials, the Partner must notify the University in writing within thirty (30) days of its receipt. Upon receipt of such notification, the University has agreed to delay enabling public disclosure of such patentable subject matter for a period not to exceed three (3) months from the date of receipt of the manuscript or presentation materials by Partner in order to file for statutory protection (the delay period may be extended for cause on a case-by-case basis with the University's concurrence). Alternatively, the author(s) shall have the option of revising the manuscript or presentation materials to avoid disclosure of the potentially patentable subject matter. Any revised manuscript or presentation materials shall be resubmitted to Partner for review, and Partner

shall continue to have the right to object on the basis of criteria specified above. Should the Partner fail to respond within thirty (30) days after its receipt of the initial manuscript or presentation material or subsequent revision thereof, the author(s) may proceed with publication or public disclosure without delay.

The PSP office will be responsible for preparing and submitting all requests, in writing, to the Partner. Primary authors will work with the PSP office to ensure that the proper submission process has been followed and that copies of all related correspondence are maintained on file. Where the primary author is not affiliated with the University, it is incumbent on the co-authors of manuscripts and presentation materials to assume responsibility for ensuring that the PSP office is included in the permissions process so that proper documentation is assured.

The PSP office will notify participants in Partner-related research of their publishing/presentation responsibilities on a regular basis.

7.2.6. Reporting of Accidental Disclosures

Should any staff become aware of an accidental disclosure of partner confidential or proprietary material, or any other security incident that could affect Partners (such as a machine compromise), a report must be made, immediately, to the Security Officer and the PSP AD. The PSP AD will be responsible for notifying the DO, who will be responsible for notifying the Office of the Vice Chancellor for Research (OVCR), who will be responsible for notifying the affected partner. This notification process will be done in a timely manner.

8. APPENDIX

8.1. DEFINITION OF TERMS

PSP AD: Assistant Director of the Private Sector Program.

Allocated systems: Computer resources where peer reviewed allocations of computing resources are made to academic researchers. Accounting is run in order to track resource usage for each user. These are typically referred to as the production compute resources or supercomputing machines.

Collaborator: A researcher working on a project with NCSA. Collaborators include Private Sector Partners, academic partners and vendors. An NCSA employee may be an NCSA collaborator for the purposes of security.

Contractual Agreement: A formal agreement between NCSA and a collaborator. Examples of these would be Operational Agreements or a Memorandum of Understanding.

DD: Division Director. NCSA Division Directors are responsible for NCSA divisions consisting of multiple teams of staff reporting to supervisors.

DO: Director's Office. The DO consists of the Director, Executive Directors, Chief Science Officer, Chief Technology Officer, and several Division Directors.

Export Controlled: Technology or documentation that is available only to permanent residents of the United States or nationals from one of the following countries: Austria, Australia, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, or the United Kingdom.

IRST: Incident Response and Security Team. The NCSA IRST is lead by the NCSA security team, and includes operations staff, network administration, and systems administrators.[AS1]

A machine room is a physical location that has controlled and limited access to administrators and staff. There are machine rooms located in most buildings NCSA occupies.

NCSA controlled area: Machine or other resource that is owned and managed by NCSA staff.

OVCR: Office of the Vice Chancellor for Research. The Vice Chancellor for Research is the senior campus officer with responsibility for advancing research at the University of Illinois at Urbana-Champaign.

PI: Principal Investigator. The PI is the project lead on work with collaborators.

PCF: The Petascale Computing Facility which houses the Blue Waters system.

Production system: These are resources that are centrally managed by NCSA and are supported 24x7x365. These machines include the email servers, web servers, file servers, and other critical infrastructure resources.

A security action is a procedure or set of procedures carried out to provide the desired level of security.

A security incident is any action or situation that violates documented procedures or which compromises, or has the potential to compromise, proprietary or otherwise sensitive information.

Sensitive materials are those things that have been identified as requiring protection (confidential, proprietary, or export controlled).

Staff includes: NCSA employees (paid or unpaid, including full-time, part-time, and students) or other individuals working on projects for or at NCSA.

User is anyone with an authorized account from NCSA Allocations to use NCSA resources.

A visitor is anyone who is present in an NCSA building or room who is not a staff member.

8.2. UNIVERSITY POLICY REFERENCES

University CIO Policy page:
http://www.cio.illinois.edu/policies/index.html

University Academic Staff Handbook
http://www.ahr.uiuc.edu/ahrhandbook/default.htm
Campus Policy and Procedure Manuals
http://www.fs.uiuc.edu/luci/

ISBN
2010 年 10 月 25 日 印刷
2010 年 10 月 25 日 發行
作成者: 장지훈, 김성호, 최윤근, 우준, 홍태영, 김성준, 이영주, 성진우, 양종원
發行人: 한국과학기술정보연구원
編輯人: 양종원
發行處: 한국과학기술정보연구원 슈퍼컴퓨팅센터 슈퍼컴퓨터인프라팀
대전광역시 유성구 과학로 335 (T. 042-869-0500)

그림

305-806 대전광역시 유성구 과학로 335 TEL.042-869-0732