Acceptable Use Policy Gap Analysis

Issue:

A statement on security and privacy was released by the Duke University Information Technology Advisory Council (ITAC) in May 1997. The document is titled **Computing and Electronic Communications at Duke University: Security & Privacy** and its stated purpose is "to establish and promote the ethical, legal, and secure use of computing and electronic communications for all members of the University community".

The document is over ten years old and only applies to Duke University and not the Duke University Health System (DUHS). It does not encompass certain legal, regulatory and compliance issues that have arisen since its inception. Additionally, the computing environment has changed significantly with ubiquitous access to the Internet and exponentially increased use of mobile computing devices allowing users to stay connected wherever they are – on or off campus.

The Information Security Steering Committee (ISSC) has been briefed on this issue and has asked to review the current policy and gaps that exist within it. A listing of identified gaps is included to further enable a dialogue with the appropriate members of the Duke constituency with the goal of creating a uniform Acceptable Use Policy (AUP). This policy should provide guidance at the highest level for Duke University and Duke University Health System as well as provide a framework for ether entity to add additional sub-components for its use.

Gaps and Proposed Remedies:

1. ***Gap: Lack of Explicitly Defined Acceptable Use Policy for Duke University and Duke University Health System:*** Duke University has viewed the existing **Computing and Electronic Communications at Duke University: Security & Privacy** statement as an AUP, although it does not explicitly carry such a title. There is no overarching policy at DUHS governing the behavior of users while utilizing Duke's computing resources. Regulations such as the HIPAA Privacy and Security Regulations require an AUP. The Duke University Office of Internal Audits has recommended the adoption of an AUP as a result of the HIPAA IT Security Governance Review they performed.

   Proposed Remedy: Rename the **Computing and Electronic Communications at Duke University: Security & Privacy** to be **Acceptable Use Policy**. Pending modification of the existing statement on security and privacy to address the issues identified herein, DUHS and Duke University should adopt the same AUP. Replace "University community" in the first paragraph of the policy with "Duke University and all of its subsidiaries, hereafter referred to as 'Duke.'" Replace all subsequent occurrences of "University" and "the University" with "Duke."

2. ***Gap: E-Discovery Amendments to the Federal Rule of Civil Procedure:*** Federal regulation governing E-Discovery went into effect after the ITAC policy was published. E-Discovery addresses the issues of legal procedure for the large percentage of information now stored electronically rather than as traditional paper records. This information may include email, word-processing files, spreadsheets, database records, web pages, electronic calendars, digital photos, videos, surveillance camera records, IM (instant messaging) transmissions, voice messages, etc. E-Discovery applies to the entire Duke constituency and can be very invasive. Duke may be required to view, access, and/or preserve user files in the course of fulfilling its legal obligation under this federal judicial ruling.

   Proposed Remedy: Insert the following text as the third sentence within the second paragraph of the existing policy: "In addition, compliance with federal or state laws, judicial rules, and/or Duke's legal interests may necessitate viewing, accessing and/or preserving system logs, network logs or user files relevant to pending or potential litigation, regardless of whether the actual user files stored on servers and/or on desktops that are owned institutionally by Duke or owned by an individual faculty/staff member, or external service provider."

3. **Gap: HIPAA Security and Privacy Regulations:** National standards for the privacy and security of individually identifiable health information, applicable to entities covered by HIPAA went into effect after the ITAC policy was published. The covered entity for Duke stretches beyond DUHS and includes Duke University, and violations can result in personal liability for individuals. As a result any compliance related concerns must be addressed holistically across Duke. The Centers for Medicare and Medicaid Services (CMS) and the Office of the Inspector General (OIG) are in the process of performing HIPAA audits on select entities. At Duke the entire covered entity is within scope – Duke University and DUHS.

   Proposed Remedy: Insert a new third sentence in paragraph 3: "In addition, users bear a personal responsibility to comply with all Duke policies, contractual obligations, and state and federal laws and regulations, including protecting the private information of others.

4. ***Gap: Digital Millennium Copyright Act:*** United States copyright law that went into effect after the ITAC policy was published. While it limits the liability of nonprofit institutions of higher education, when they serve as online service providers, its copyright infringement provisions apply to staff and faculty members. We have been seeing an increase in complaints directed at faculty and staff members. Related, the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) use of "preservation notices" in some cases compels Duke to save specific network logs identifiable to an individual user.

   Proposed Remedy: Partially covered by proposed changes to 2) above. Insert ", network transmissions" to the penultimate sentence of the second paragraph so that it reads: "…the ultimate privacy of messages, network transmissions and files cannot…"

5. ***Gap: Expanded Use of Duke Credentials:*** There has been a growing trend toward the sharing of user IDs and passwords. This is becoming more problematic as these credentials are used to logon to new tools like employee self service that gives one access to payroll data, investment data and other personal data. DHTS has promulgated a statement regarding account and password privacy called the **Duke Medicine Password Standard** that addresses password sharing.

   Proposed Remedy: Insert a new stand-alone paragraph after the existing second paragraph adapted from the **Duke Medicine Password Standard**: "An account owner should not reveal a password to an IT support technician or any other individual, even though they may claim to work for the IT service (over the phone or in person). If, in the professional judgment of the user, it is necessary to share a password with an IT support technician or any other individual, the password must be changed as soon as possible thereafter. Once shared, a password is considered compromised and must be changed immediately."

6. ***Gap: NC Identity Theft Protection Act:*** This North Carolina regulation went into effect after the ITAC policy was published. The purpose of the regulation is to prevent or discourage identity theft as well as the safe guarding and protection of individual privacy. It was designed to restrict the use of an individual's social security number and to protect the encoded information on credit, debit and other cards with consumer and financial information.

   Proposed Remedy: Covered by proposed changes to 3) above.

7. ***Gap: Payment Card Industry Data Security Agreement (PCI DSS):*** The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. It went into effect after the ITAC policy was published and is a very comprehensive and prescriptive standard that is intended to help organizations proactively protect customer account data.

   Proposed Remedy: Covered by proposed changes to 3) above.