

University of New Hampshire

University of New Hampshire Scholars' Repository

Faculty Senate Motions

Faculty Senate Documents

12-9-2019

UNH FACULTY SENATE MOTION # XXIV – M4 that IT services of USNH should fully follow the NIST SP 800-63B guidelines

Faculty Senate

Follow this and additional works at: https://scholars.unh.edu/faculty_senate_motions

Recommended Citation

Faculty Senate, "UNH FACULTY SENATE MOTION # XXIV – M4 that IT services of USNH should fully follow the NIST SP 800-63B guidelines" (2019). *Faculty Senate Motions*. 79.
https://scholars.unh.edu/faculty_senate_motions/79

This Text is brought to you for free and open access by the Faculty Senate Documents at University of New Hampshire Scholars' Repository. It has been accepted for inclusion in Faculty Senate Motions by an authorized administrator of University of New Hampshire Scholars' Repository. For more information, please contact Scholarly.Communication@unh.edu.

**UNH FACULTY SENATE
MOTION # XXIV – M4**

that IT services of USNH should fully follow the NIST SP 800-63B guidelines

1. Motion presenter: Michel Charpentier, on behalf of the Information Technology Committee
2. Date of Faculty Senate Discussion: 11/25/2019 and 12/09/2019

3. Rationale: In their meetings with the Faculty Senate IT Committee, the UNH IT Security Committee and the new USNH CIO emphasized the extreme importance of security. During these discussions, they relied on the "Digital Identity Guidelines: Authentication and Lifecycle Management" (NIST SP 800-63B) document recently produced by the National Institute of Standards and Technology (NIST), and used this document to justify ongoing and future efforts to improve the overall security of the UNH/USNH IT infrastructure. NIST is responsible for developing information security standards and guidelines for federal agencies. The NIST SP 800-63B document provides recommendations on types of authentication processes.

The Faculty Senate IT Committee agrees with the UNH IT Security Committee and the USNH CIO on the importance of security and welcomes the choice of NIST SP 800-63B as the standard to follow when IT security-related decisions are made at UNH. We observe, however, that the latest changes to UNH IT procedures have not been following these guidelines consistently. For instance, faculty were recently notified of a new USNH Password Policy that requires faculty members to use passwords with a length between 14 and 64 characters and mandates that these passwords be changed every year. This is not consistent with NIST SP 800-63B, sections 5.1.1.2: "Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)" and 10.2.1: "Do not require that memorized secrets be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise".

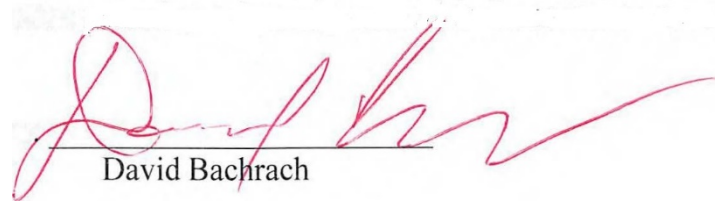
The NIST guidelines were developed by experts in security and are deemed suitable by a wide range of federal agencies. Their authors understand the complex interactions in which activities from all participants in an IT system interplay, and how decisions that initially make sense intuitively can end up being counterproductive. For instance, impaired usability in the name of better security can end up making systems less secure: "poor usability often results in coping mechanisms and unintended work-arounds that can ultimately degrade the effectiveness of security controls.[...] Positive user authentication experiences are integral to the success of an organization [...]. The overarching authentication usability goal is to minimize user burden." (NIST SP 800-63B, section 10). UNH should leverage the expert work that went into the creation of guidelines like NIST SP 800-63B, and not second-guess their conclusions without valid reasons to do so.

In addition to being detrimental to security, variances from NIST procedures can result in increased cost to the university. For example, regular password changes on multiple devices often trigger lockouts. IT help desk statistics show that there were approximately 1344 lockouts between 7/1/2018 and 9/30/2019. These lockouts take time away from the primary duties of faculty and staff.

4. Motion: All IT services of USNH should fully follow the NIST SP 800-63B guidelines to ensure the digital security of faculty, staff and students. Any deviation from these guidelines should be considered only in extraordinary circumstances and the decision to deviate should be substantiated with comparative data.

5. Senate action: The motion passed with 51 in favor, none opposed, and 1 abstention.

6. Senate chair's signature:



David Bachrach

Forwarded to the following on February 18, 2020:

President James Dean
Provost Wayne Jones
Bill Poirier, Chief Information Officer, UNH and USNH