Medical University of South Carolina

Policies and Procedures Governing E*Value Account Creation and Maintenance

Authors:
Marna Stilley (OCIO)
Mitchelle Morrison (OCIO)
Alicia Martinez (GME Office)
Lawrence Afrin, M.D. (GME Office)

Policies

1. To enhance security, **MUSC users** of E*Value needing to manually login to E*Value will access the system by entry of their **MUSC trusted account** (e.g. NetID) at the **MUSC E*Value portal**. MUSC users of E*Value will not login to E*Value via an E*Value vendor issued account (i.e. not through the vendor's home page). The E*Value vendor issued password will be revoked for MUSC users, and MUSC users will not be able to **re-enable** their E*Value vendor issued password.

2. The **E*Value superuser** for each MUSC college will bear primary responsibility (and OCIO will bear secondary responsibility across all colleges) for ensuring **MUSC users** (both existing and new) of E*value in their purview comply with policy 1 by virtue of ensuring that (1) the E*Value vendor issued account is properly matched up to the afore mentioned MUSC trusted account, and (2) the E*Value vendor issued password has been revoked (or not setup) and not reset. Each college's superuser (and OCIO) may establish procedures appropriate to that college (or OCIO) to ensure this responsibility is met; the E*Value Superuser Committee must be kept informed of all such procedures (and updates), which will be incorporated into the Committee's minutes.

3. Each college's E*Value superuser will be responsible for presenting evidence of compliance with policies 1 and 2 above to the **E*Value Superuser Committee** at least annually. Such evidence will be incorporated into the Committee's minutes. The OCIO team designated by the **MUSC OCIO Director of Academic and Research Computing** will support the E*Value superusers and the committee as needed.

4. New E*Value users must comply with policy 1. New MUSC users of E*Value must follow the policies and procedures of the appropriate MUSC trusted Identity Provider. Only after the account has been issued by the appropriate MUSC trusted Identity Provider may the matching E*Value issued account be setup. Only the E*Value superusers are authorized to create E*Value accounts. Said E*Value superuser are responsible for ensuring that a user is not entered more than once (for example as both an account matched to the MUSC trusted account and one that is un-matched).

5. The E*Value superuser for each MUSC college is responsible for ensuring all program administrators in that college are kept informed of these policies and related procedures (and updates).

6. Upon termination, an MUSC user of E*Value should be either inactivated or converted to a non-MUSC account by un-matching the E*Value account from the MUSC trusted account. A non-MUSC user can be issued an E*Value password.

Procedures

1. The E*Value account is matched to the MUSC trusted account by filling in the NetID field with the user's NetID per the MUSC IDMS system. **myDirectory** is a useful tool for this purpose. Should the NetID userid change, follow the NetID change notification procedure. **Check accounts** is a useful tool for determining if a NetID userid is active and valid.

2. The E*Value vendor will seek to disable the system's "Password Change" functionality for users whose accounts bear a populated MUSC NetID field. Compliance with policy 1 can be verified by determining that the user's password field has been cleared.

3. The E*Value superuser for each MUSC college is responsible for determining the appropriate template and procedure to use when creating accounts. Each college is responsible for publishing their procedures.

4. Unmatching an MUSC user account from the MUSC trusted account requires the email address field be changed to a non-MUSC issued email address and the NetID field be cleared. An E*Value password is then issued.

Definitions

1. **MUSC trusted Identity Provider** - MUSC's Identity Management System (IDMS) provides NetID's for all MUSC approved users. MUSC is a member of the [InCommon Federation](#) and trusts the Identity Provider of other members of the InCommon Federation. The University of South Carolina (USC) is also a member of the InCommon Federation. The South Carolina College of Pharmacy (SCCP) faculty, staff, and students located at USC could use their USC Network Username and password in compliance with policy 1, if it were technically possible. Thus until such time as it is technically possible, the SCCP faculty, staff, and students located at USC are considered non-MUSC users for the purposes of E*Value.

2. **MUSC user** - A user entitled to a network account issued by an MUSC Identity Provider or an Identity Provider trusted by MUSC, with the exception noted above.

3. **MUSC trusted accounts** are the MUSC NetID issued by the [MUSC trusted Identity Provider](#) and accounts issued by InCommon Federation Identity Providers.

4. **E*Value superuser** – A user designated by an MUSC college as principally responsible for overseeing all E*Value operations within the college. Each MUSC college using E*Value appoints at least one E*Value superuser. Most MUSC colleges will have only a small number (one or two) of E*Value superusers appointed. The dean of the college, or his/her designate, is responsible for appointing the college's E*Value superuser(s).

5. [**MUSC OCIO Director of Academics and Research Computing**](#)

6. **E*Value Superuser Committee** – The institutional-level committee comprised of all E*Value superusers from across the institution. The chair, who may or may not be an E*Value superuser, is appointed by the Associate Provost for Education and Student Life. The E*Value Superuser Committee meets regularly to review institutional-level issues related to E*Value.