Business Manage Users Service Agreement

1. Definitions

“Manage Users Service.” The Manage User Service allows “Managing Users” or "Business Admin's" to add or remove “Users” and to add, edit, and remove User permissions within a member business’s Digital Banking. “User or Sub User.” User means any individual authorized and able to access your Digital Banking, regardless of any restrictions or limitations on the User’s use of functionalities or services (“permissions”) within your Digital Banking. New Users created within the Manage Users Service are selected at the discretion of the Managing User(s). New Users need not have any pre-existing authorization to access accounts or transact on behalf of the member business. New Users may be created with the ability to act as Managing Users, including the ability to create additional new Users. At first log-in, each new User will be required to agree to the UICCU Digital Banking Agreement and establish new Access Credentials that are personal and specific to that User, including username and password. “Managing User.” For purposes of this Agreement and Service, a Managing User is any User of a member business’s Digital Banking who uses the Manage Users Service. “Role.”

A Role is a selection of available Digital Banking service permissions and transaction limitations to be assigned to a User. A Role or Roles must be created first. Users may then be created and assigned a Role. “Business Admin role.”

The Business Admin role includes all Manage Users permissions and is granted to the member business at Digital Banking registration and to authorized account signers by UICCU staff. Users with the Business Admin role may assign Manage Users and Manage Roles permissions to new Roles and assign those Roles to new Users.

2. Creating Roles within the Service

CAUTION: Roles created within the Manage Users Service should only be entrusted to carefully selected individuals who are at least 18 years of age. By accepting this Agreement and by using the Manage Users Service, you acknowledge the risk of authorizing new Users to independently manage accounts, accept service agreements and disclosures, and transact on your behalf within Digital Banking, and you agree that the value of the Service to you outweighs such risk. You further accept and agree that you must exercise due care and well-informed business judgment when creating Roles, creating Users, and assigning Roles to Users. Due care and the exercise of well-informed business judgment includes a review of the user guides, FAQs, best practices guides, “tool tips,” and disclosures provided by UICCU.

A Role may include any or all permissions presented in the Manage Users Service. UICCU reserves the right to remove or add any listed activities and available permissions at any time. Standard permissions available in the Manage User Service may include the following:

a. **Accounts Selection:** The Managing User selects the accounts that the User will be granted permission to view balance, view transaction history, and export transactions.
b. **Business Credit and Debit Cards:** A Managing User may select any or all of the following permissions regarding debit or credit cards associated with the accounts selected by the Managing User:

    - Report Lost or Stolen Card
    - Request New Card

- Advanced Card Controls
- Change Debit Card Pin
- Activate Card

NOTE: There is a potential for card abuse when a User you do not intend to authorize to transact with the debit or credit card is nonetheless granted the ability to manage the credit or debit card. Before creating a Role with these permissions, carefully consider the business needs and qualifications of the individual Users to whom the Role will be assigned. ANY CARD MANAGEMENT, CARD CONTROL, OR CARD ACCESS PERMISSIONS GRANTED TO A USER THAT ENABLE THE USER TO TRANSACT ON A CARD, DIRECTLY OR INDIRECTLY, SHALL CONSTITUTE YOUR AUTHORIZATION OF THE USERS' TRANSACTIONS.

c. External Account Transfers: A Managing User may create a Role that includes permissions to create, view, and manage ACH transfers from your selected UICCU accounts to other UICCU accounts or to accounts held at other financial institutions and identified in advance by the member business.

A Managing User may select any or all of the following permissions:

- View External Accounts
- Add External Accounts
- Create User to User Transfers
- View Member to Member Accounts
- Add Member to Member Accounts

The Managing User then sets a dollar limit for credit transfers and a dollar limit for debit transfers before selecting those internal accounts that the User may credit and those that the User may debit.

d. Transfers: A Managing User may permit users to transfer funds to and from the member business's UICCU accounts. Depending on the other permissions granted, a User may be able to use this permission to transfer funds from a UICCU account to an external account.

e. Business ACH: If the member business has enrolled in the Business ACH service, which is part of UICCU's CASH Management program, a Managing User may select from the Business ACH features listed below and establish daily and monthly dollar limits for Business ACH transfers, as well as a dollar limit for Same Day ACH transfers.

- Add ACH Templates
- Approve ACH Templates
- Delete ACH Templates
- Access Restricted Templates
- Import ACH Templates
- Schedule Same Day ACH
- ACH History
- ACH Reversals
- Manage ACH NOCs (Notification of Change) and Returns
- Add Recipient
- Delete Recipient

f. Wire Transfers: If the member business has enrolled in our Wire Transfer service, a Managing User may specify the account to be used for Wire Transfers by submitting their request via a secure form.

g. **Manage User**: A Managing User with the Business Admin role may create a role with any or all of the following permissions. Note that dual approval from the Business Admin will be required if a Managed User creates a new user and/or role.
    - Create Users
    - Delete Users
    - Unlock Users
    - Update Users
    - Reset Passwords
    - Deactivate Passwords

    Managed Users may create additional users, however, this will require authorized approval from the Business Admin before permissions will be active.

    NOTE: There is a potential for account abuse when a User is granted permission to independently create additional Users. Before creating a Role with these permissions, carefully consider the business needs and qualifications of the individual User to whom the Role will be assigned. IN PARTICULAR, YOU UNDERSTAND, ACKNOWLEDGE, AND AGREE THAT A USER GRANTED (1) CREATE USER, (2) ASSIGN ROLE, AND (3) VIEW ROLE PERMISSIONS, TOGETHER, WILL HAVE THE INDEPENDENT ABILITY TO CREATE NEW USERS AND THAT ANY AND ALL ACTIVITY WITHIN YOUR DIGITAL BANKING ACCOUNT BY ANY USERS CREATED WITHIN YOUR DIGITAL BANKING ACCOUNT SHALL BE DEEMED FULLY AUTHORIZED BY YOU.

h. **Manage Roles:** Any Managing User may be assigned a role including permissions to take the following actions:

    - View Users and Roles
    - Create Roles*
    - Edit Roles **
    - Assign Roles***
    - View Role Account Permissions
    - View Role External Account Permissions
    - Edit Role Account Permissions ****
    - Edit Role External Account Permissions ****

    **Only Managing Users with the Business Admin role may create additional roles with any Manage Roles permissions, but any User with Assign Roles permission can assign any role, including those with Mange Role permissions, to any other User.*

    ***Only Managing Users with the Business Admin role can edit Manage Users or Manage Roles permissions within existing roles. Other Users granted Edit Roles permission may edit all permissions EXCEPT Manage Users or Manage Roles permission.*

    ****SPECIAL CARE SHOULD BE TAKEN WHEN GRANTING THE "ASSIGN ROLES" PERMISSION. Managing Users may be unable to see all of the accounts accessible under roles that they assign to new users, depending on the restrictions of Managing Users' own roles. Managing Users unable to view all accounts remain responsible for confirming that each role they assign is appropriate for the intended user. Clear business policies and procedures regarding roles and role assignments are strongly recommended.*

    *****A Managing User may not create or edit a role in a way that grants more permissions or higher transaction limits than the Managing User has themselves.*

NOTE: There is a potential for account abuse when a User is granted permission to manage existing Roles or create new Roles. Before creating a Role with these permissions, carefully consider the business needs and qualifications of the individual User to whom the Role will be assigned. IN PARTICULAR, YOU UNDERSTAND, ACKNOWLEDGE AND AGREE THAT A USER GRANTED (1) CREATE USER, (2) ASSIGN ROLE, AND (3) VIEW ROLE PERMISSIONS,TOGETHER, WILL HAVE THE INDEPENDENT ABILITY TO CREATE NEW USER AND THAT ANY AND ALL ACTIVITY WITHIN YOUR DIGITAL BANKING ACCOUNT BY ANY USER CREATED WITHIN YOUR DIGITAL BANKING ACCOUNT SHALL BE DEEMED FULLY AUTHORIZED BY YOU.

3. Member Business Policies

You agree that the following measures are prudent, commercially reasonable, and will be adopted as policies or procedures of the member business relating to use of the Manage Users Service:

a. Review any FAQs, or disclosures provided by UICCU before assigning a role to a User. If you have any questions about the Manage Users service, you will contact a UICCU representative in branch or at 217-278-7700 for more information before a User is activated.
b. Assess the trustworthiness of all Individuals to be designated as Users according to best practices or applicable industry standards. *(UICCU recommends that all Users be subject to background checks.)* Assign Roles to each individual User using due care and well-informed business judgment regarding the operational needs, qualifications, and trustworthiness of the individual User.
c. Immediately deactivate a user during any significant period of leave of absence from the business, such as due to extended illness, parental leave, or sabbatical.
d. Immediately delete a User whenever the User's relationship with the member business terminates for any reason, and immediately reassign a User to an appropriate Role whenever the User no longer has need for the access and permissions originally granted through the Manage Users Service.
e. Actively monitor the phone numbers and email addresses you provided as your contact information for alerts and notifications from the Manage User Service.

4. Limitation of Liability

YOU UNDERSTAND AND AGREE TO SELECT AND AUTHORIZE ALL USERS ENTIRELY AT YOUR OWN RISK. SELCO SHALL HAVE NO LIABILITY FOR ANY ACTS OR OMISSIONS OF YOUR USERS, INCLUDING ANY ACTION, INTENTIONAL OR UNINTENTIONAL, BY A USER THAT CIRCUMVENTS OR EXCEEDS THE LIMITATIONS OF THE ROLE ASSIGNED TO THE USER. EXCEPT AS OTHERWISE PROVIDED IN THIS AGREEMENT OR AS REQUIRED BY LAW, SELCO SHALL IN NO EVENT BE LIABLE, WHETHER IN CONTRACT, WARRANTY, TORT, OR OTHERWISE, FOR ANY ACTUAL, DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, LIQUIDATED OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, OR BUSINESS, ARISING IN WHOLE OR IN PART FROM YOUR USE OF THE MANAGE USERS SERVICE OR THE ACTS OR OMISSIONS OF YOUR USERS.

5. Security of Access Credentials

Each User is responsible for safeguarding his or her personal Access Credentials. UICCU is entitled to act on transaction instructions within the scope of the permissions assigned to a User and received using valid User Access Credentials. The User's Access Credentials will have the same effect as the User's signature. If a User fails to maintain the security of his or her Access Credentials and fraudulent charges or activity occur on your account, you will be liable for the full amount of the charges unless prohibited by

law. If a User fails to maintain the security of his or her Access Credentials and UICCU suffers a loss, UICCU may immediately terminate the User's access, and your access, to Digital Banking.

You agree to notify us, according to UICCU's notification requirements, if you believe a User's Access Credentials have been stolen, compromised, or otherwise become known to unauthorized persons. UICCU shall have no liability for any transactions until we have received and had a reasonable opportunity to act upon such notice from you unless liability is specifically assigned to UICCU by law or regulation.

6. **Notices and Alerts**

When certain actions are taken within the Manage User Service, notices or alerts may be automatically generated and sent to the member business email address and/or phone number on file. It is your responsibility to ensure that the email addresses and phone numbers we have on file are operational and routinely monitored by appropriate representatives of the member business.

7. **Application of Other Agreements**

You understand and agree that all acts or omissions of your Users are attributable to you, and the terms of all of your UICCU agreements, including, but not limited to, the Digital Banking Agreement and UICCU Membership and Account Agreement, shall apply to the acts or omissions of your Users as if they were your acts or omissions.

8. **Indemnification**

You agree to indemnify and hold UICCU, its officers, directors, shareholders, agents, employees, and affiliates, and an affiliates' respective officers, directors, agents and employees, harmless from and against any and all third-party claims, suits, losses, costs, damages, liabilities, or expenses (including reasonable attorneys' fees) arising from or related in any way to (i) any Services performed in connection with this Manage Users Agreement, (ii) UICCU's action or inaction in accordance with or in reliance upon any instructions or information received from you, your User, or anyone using your User's access credentials, (iii) your or your User's breach of any of your representations, agreements, responsibilities, or warranties made under this Agreement, within the Manage Users Service, or otherwise related to the Manage Users Service; (iv) your or your User's breach of applicable laws, rules or regulations; and (v) any action by you or your User to circumvent or exceed the limitations of the Role assigned to the User

9. **Disclaimer of Warranties**

YOU UNDERSTAND AND AGREE THE MANAGE USERS SERVICE IS PROVIDED AS-IS AND THAT USE OF THE SERVICE SHALL BE AT YOUR OWN RISK. TO THE FULLEST EXTENT PERMITTED BY LAW, SELCO DISCLAIMS ALL REPRESENTATIONS, WARRANTIES AND CONDITIONS OF ANY KIND (EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT OF PROPRIETARY RIGHTS) AS TO THE MANAGE USERS SERVICE AND ALL INFORMATION, PRODUCTS, AND OTHER CONTENT (INCLUDING THIRD PARTY INFORMATION, PRODUCTS AND CONTENT) INCLUDED IN OR ACCESSIBLE THROUGH OR A RESULT OF THE MANAGED USER SERVICE. SELCO DOES NOT WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE, OR THAT DEFECTS WILL BE CORRECTED. YOU UNDERSTAND AND AGREE THAT DESPITE ANY PREVENTIVE ACTIONS BY YOU OR SELCO, THE PERMISSIONS AND LIMITATIONS YOU ATTEMPT TO APPLY WHEN CREATING A ROLE WITHIN THE MANAGE USERS SERVICE MIGHT BE INTENTIONALLY OR UNINTENTIONALLY EXCEEDED OR CIRCUMVENTED. SELCO MAY DISCONTINUE THIS SERVICE AT ITS SOLE DISCRETION.

10. **Fees**

UICCU reserves the right to assess fees for the Service, with notice to you as and when required by law. The current Business Rate and Fee Schedule may be viewed here: Business Rate and Fee Schedule.

11. Dispute Resolution; Governing Law

The parties hereby agree that any dispute concerning this Agreement, or the Financial Wellness Service, will be resolved in accordance with the procedures contained in the University of Illinois Community Credit Union Digital Banking Agreement and other agreements referenced therein, including the UICCU Community Credit Union Membership and Account Agreement, and that the dispute resolution, arbitration clause, and governing law provisions of such agreements will apply with equal force to this Agreement.

12. TCPA Opt-In

UICCU may contact you from time to time such as if we identify opportunities to save you money, add convenience to your credit union experience, or in the event of fraud. In accordance with the Telephone Consumer Protection Act (TCPA), UICCU must obtain consent before contacting your cell phone to discuss certain types of account activity. By agreeing to the terms and conditions below, you grant UICCU permission to contact you at the telephone numbers you have provided to the Credit Union. This may include contact via an auto-dialing and/or prerecorded message, text message, or standard call. You have the right to opt-out of this permission at any time by contacting the Credit Union to revoke consent via phone (217-278-7700) or a secure message through you digital banking.

13. SYSTEM REQUIREMENTS

The minimum encryption requirement for accessing credit union account(s) online is TLS 1.3 protocol with forward secrecy and 128-bit (or higher) encryption ciphers, which are the supported defaults for these operating systems, browsers, and versions.

In addition, JavaScript must be enabled, web extensions must be disabled, ensuring the most optimal experience.

Supported Operating Systems and Browers

Vendor Operating System	Browser
Microsoft Desktop = Windows 11 or higher, Mobile = N/A	Edge (last two versions)
Apple Desktop = Mac OS 11 or higher	
Apple Mobile/Tablet = iOS (last two versions)	Safari (last two versions)
Google Mobile/Tablet = Android 13.0 or Higher	Chrome (last two versions)
Mozilla Desktop = N/A,	Firefox (last two versions)