

Adding Additional Date Fields

Clients can now create additional custom date fields within CU PolicyPro and RecoveryPro. The additional date fields will work exactly like the system-defined date fields and will show on the printed/published versions of the content. Clients can use their custom fields along with or instead of the system-defined date fields. If an Additional Date Field does not have a date entered, it will not show on the printed/published content.

You can add these additional custom date fields by navigating to the settings area and clicking the Edit Icon next to Custom Date Fields:

Home	My 360 View	InfoSight	CU PolicyPro	RecoveryPro	Resources	CU Documents	Discussion Board	Admin
System Admin:Name			No					
Default Font			No					
Deafult Font Header			No					
Deafult Font Body			No					
Admin Login Type			No					
Custom Date Fields			No					

Pop Up Screen #1 will appear. Click the “Add Field” button

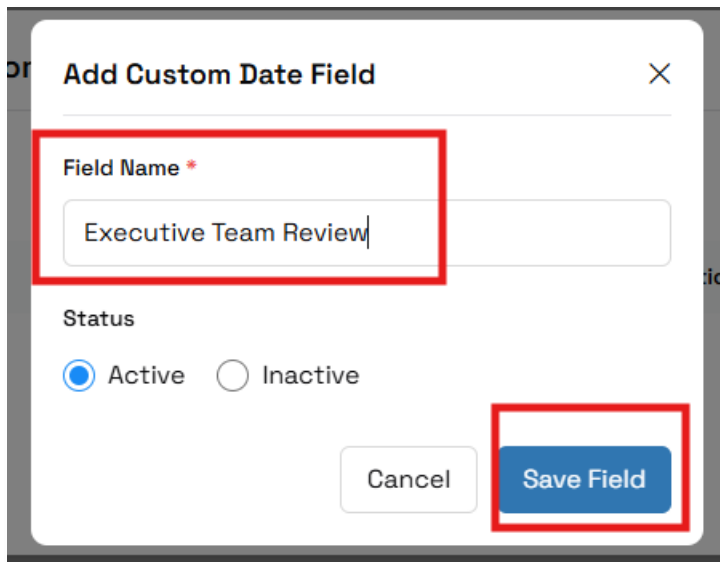
Manage Custom Date Fields

+ Add Field

Order	Field Name	Status	Actions
No custom date fields added yet.			

Close

Pop Up Screen #2 will appear. Enter the label for the date field and click the “Save Field” button:



Add Custom Date Field [X]

Field Name *

Executive Team Review

Status

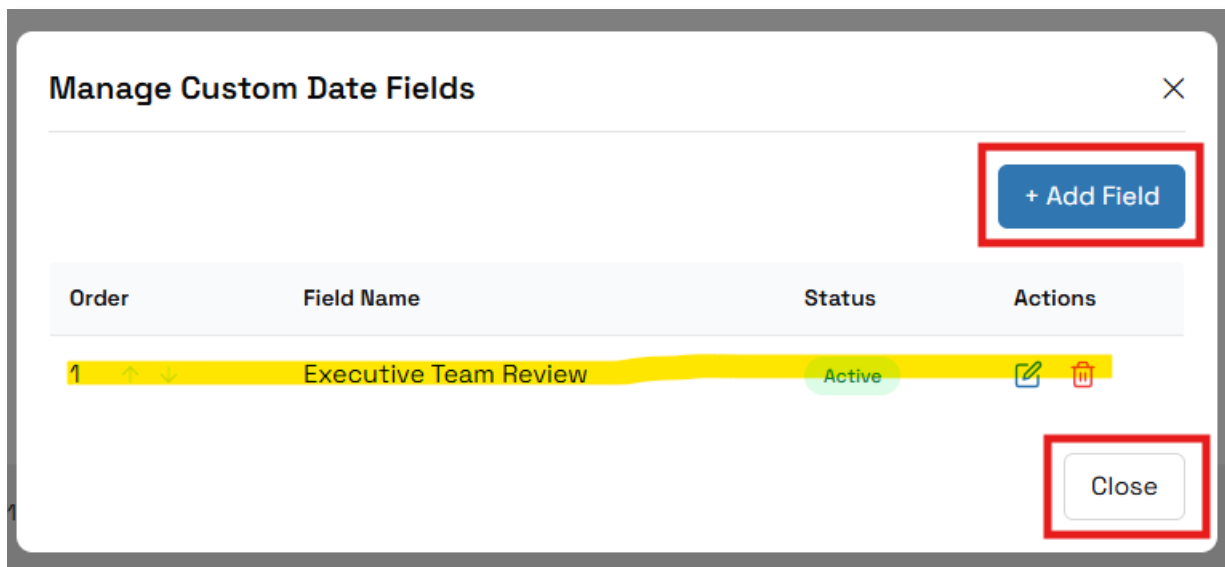
☒ Active ☐ Inactive

Cancel Save Field

You will be returned to Pop Up Screen #1 where you can review your entry.

To add additional fields click the “Add Field” button again.

To save the newly created field(s), click on the Close button.



Manage Custom Date Fields [X]

+ Add Field

Order	Field Name	Status	Actions
1	Executive Team Review	Active	

Close

On the editing screen the Additional Date Field(s) will show directly below the content editing area.

Note: If no custom fields have been created, the Additional Date Field area will not show.

know how and to whom to report the activity. This training will be conducted both before and after the Incident Response Plan. General training and specialized training shall occur upon hire or in

P. Incident Response Testing.

- i. Management will test the effectiveness of the incident response plan. Examples are limited to, the following:

1. Employee reports suspicious email (i.e. phishing)

Additional Date Fields

Executive Team Review

MM/DD/YYYY



Model Content Information

Incident Response is a **mandatory** policy. ([NCUA 748](#))

Credit unions are also encouraged to utilize the [FFIEC Cybersecurity Assessment Tool](#).

You will see your new custom date fields when you print preview, print, or publish your document.

Policy 4125 : Incident Response

Print

Close

Revised Date: 06/22/2026

Reviewed Date: 06/23/2026

Executive Team Review: 06/13/2026

Note: While CU PolicyPro does not contain a Cybersecurity Policy per se, Policies 4120 and 4125 used together fulfill cybersecurity policy expectations. It is also important to note that Policy 4120 is more than a cybersecurity policy, in that it includes physical security and other, non-'cyber' security considerations.

Model Policy Revised Date: 12/24/2024

General Policy Statement:

MCUL 2026 (Credit Union) recognizes its responsibility to safeguard member information and will treat the private financial information of the Credit Union's members ("member information") with appropriate care to maintain the confidentiality, integrity and security of member information. The Credit Union will ensure that incidents of unauthorized access to member information are addressed immediately, including notice to the membership as well as the proper authorities. The purpose of this policy is to set forth the guidelines for management and staff to use in establishing and maintaining policies and procedures to address incidents of unauthorized access to member information. The Credit Union will comply with all applicable laws and regulations governing the safeguarding of member information including NCUA Guidelines for Safeguarding Member Information (12 CFR Part 748 Appendices A and B, Part 749 Appendix B) (the "Guidelines") and all other applicable laws and regulations regarding the safeguarding of member information.

Definitions:

- **Compromise** means the unauthorized disclosure, modification, substitution, or use of sensitive data or the unauthorized modification of a security-related system, device, or process to gain unauthorized access.