FrontierZero

Hubspot User Removal Guide

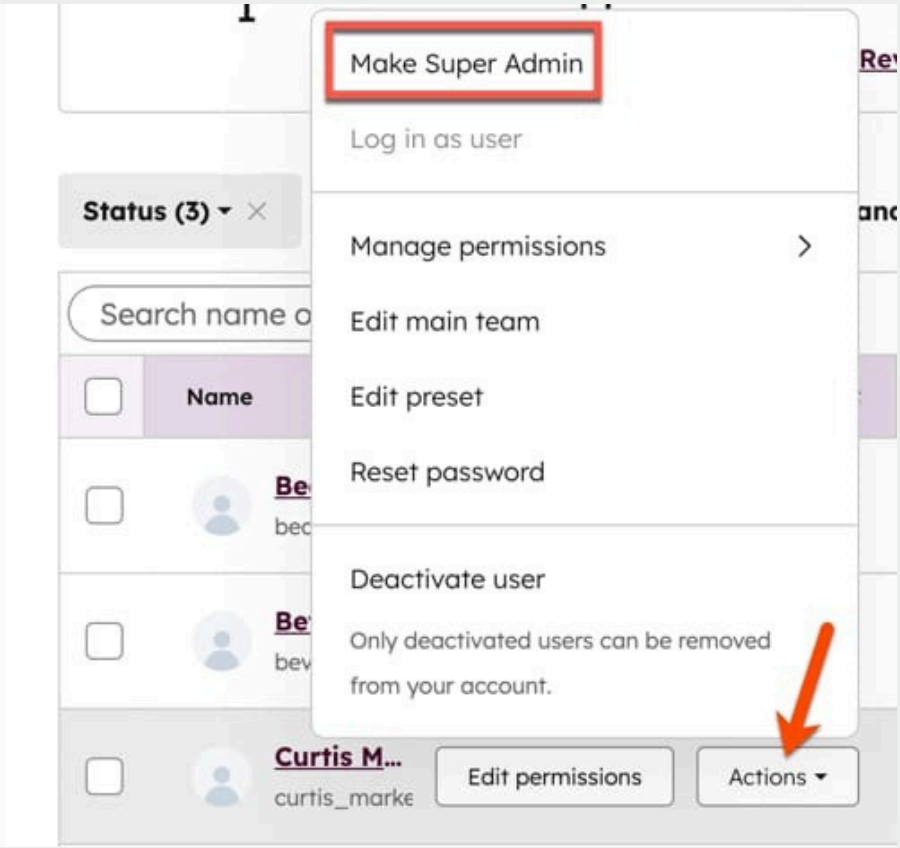
FrontierZero Customer Security Guide
March 2026

Executive Summary

Managing HubSpot user access requires a systematic approach that prioritizes security while maintaining operational continuity. As a cybersecurity company, FrontierZero recommends complete user removal as the default best practice to minimize the attack surface and reduce potential security risks. This guide outlines the critical differences between user deactivation and removal, provides a comprehensive pre-removal checklist, and establishes security best practices for HubSpot CRM operations.

Key Takeaway: Complete user removal should be the default action for enhanced security. Every inactive account represents a potential vulnerability that threat actors can exploit. Deactivation is only a temporary measure during the transition period.

Understanding Deactivation vs Removal



When it comes to removing a departing user from HubSpot, you have two options, but they are not equal.

Deactivation is a temporary state that preserves access pathways and leaves your account exposed. Complete removal eliminates the threat entirely.

The next page breaks down exactly what happens with each approach, and why one should always be your default.

Deactivation (Temporary Transition Only)

What happens:

- The user cannot log in or access the account
- User prole remains intact in the system
- Historical data and ownership are preserved for reporting
- The user can be reactivated later with all current assets
- Notifications stop immediately
- Paid seat retained, but doesn't count toward seat total
- User remains visible in the Sales Forecast tool

Security Risk: Deactivated accounts still exist in the system and can be reactivated. If credentials are compromised or an attacker gains administrative access, these accounts can be exploited.

Use deactivation only as a temporary measure:

- 72-hour transition period while reassigning assets and updating workflows
- Short-term contractor pause (less than 30 days expected return)
- Emergency access suspension pending investigation

Complete Removal (Recommended Security Practice)

What happens:

- User must be deactivated first (mandatory prerequisite)
- User prole was completely deleted from the account
- Unassigned from conversations, records, and assets
- Removed from reports and filters
- Cannot be restored—must recreate user from scratch
- Shows as "Deactivated/Removed (email)" in ownership fields
- Scheduling pages deleted permanently
- **Eliminates the account as a potential attack vector**

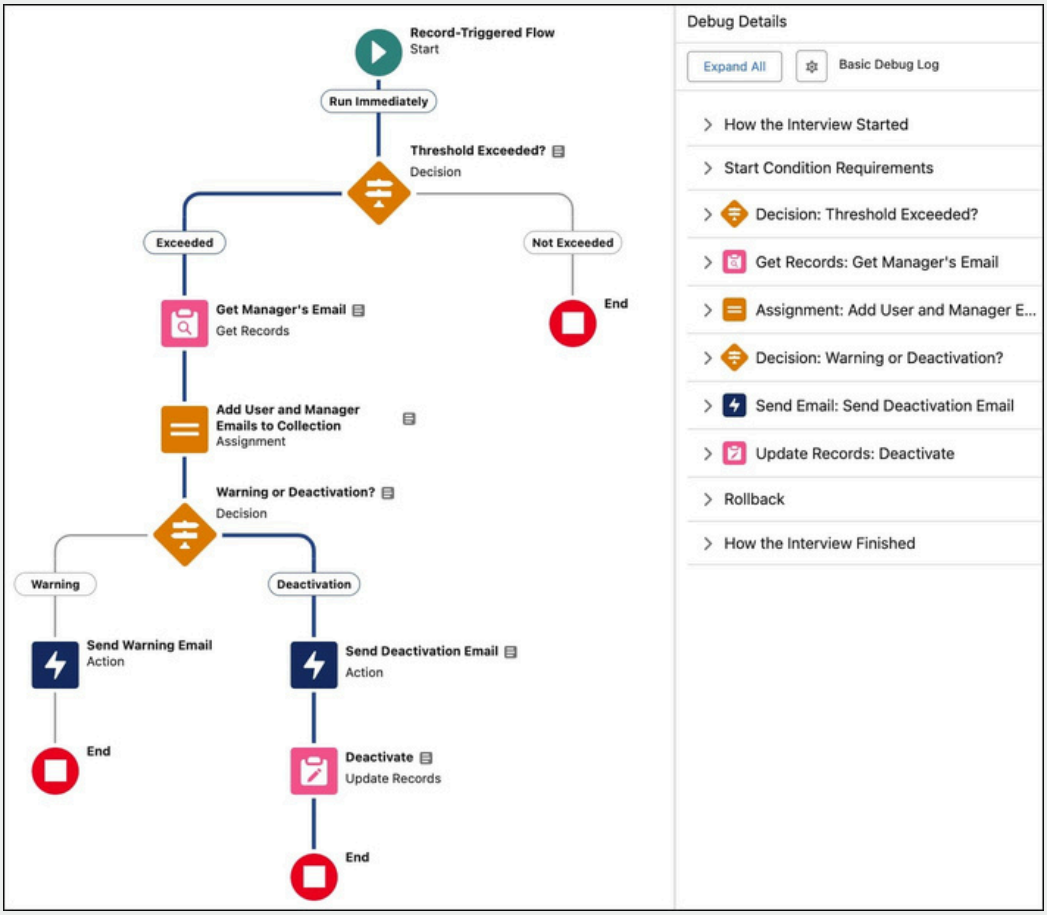
Security Benefits:

- Reduces credential theft risk
- Minimizes privilege escalation opportunities
- Limits lateral movement pathways
- Decreases the overall attack surface
- Aligns with the principle of least privilege
- Supports zero-trust architecture

Use complete removal for (default recommendation):

- Any employee who has permanently left the organization
- Contractors whose engagements have concluded
- Any account inactive for more than 72 hours
- Role changes where a new account with appropriate permissions should be created

Security First Pre Removal Checklist



Complete these steps before deactivating any user to ensure operational continuity and maintain security posture:

1. Record Ownership Transfer

- **Contacts**: Bulk reassign to active owner via object dashboard filters
- **Companies**: Transfer ownership using bulk edit
- **Deals**: Critical—lter for open deals only and reassign immediately
- **Tickets**: Reassign active tickets to appropriate team members
- **Conversations**: Review and transfer inbox assignments
- **Tasks**: Reassign open tasks to ensure follow-through

Pro tip: Filter by deal stage to identify only open deals requiring reassignment—closed deals can remain for historical reference.

2. Automation and Workflow Updates

- **Workflows**: Use HubSpot's nd/replace feature to swap user references in workflow criteria and actions
  - Navigate to Settings → Users & Teams → Select user → Review user's records and assets → Workflow configurations → View All → Replace

- **Rotation owners**: Remove from record owner rotation actions
- **Sequences**: Check for active sequence enrollment and scheduled emails
- **Task automation**: Update any automated task assignment rules
- **List filters:** Review lists using the user as criteria

3. Meetings and Scheduling

- **Scheduling pages:** Turn off or transfer personal scheduling links
- **Round-robin meetings:** Remove from group scheduling rotations
- **Meeting links:** Update any shared meeting links in email signatures or website

Warning: Scheduling pages will be permanently deleted upon user removal—transfer ownership before deactivation.

Security Note: Orphaned scheduling links can be exploited for reconnaissance or social engineering attacks. Ensure all external-facing booking links are disabled immediately upon employee departure

4. Paid Seats and Permissions

- **Paid seat removal:** Unassign Sales Hub, Service Hub, or Marketing Hub seats before deactivation
- **Permission sets:** Check and remove any custom permission assignments•
- **Role assignments:** Update team roles and hierarchies
- **API keys and tokens:** Revoke any personal API keys or access tokens associated with the user
- **Integration accounts:** Disconnect any third-party integrations tied to user credentials

Security Note: Deactivated users retain their permission structure. If the account is compromised and reactivated, those permissions are immediately restored. Remove all privileges before deactivation.

5. Account and Billing Roles

- **Primary Account Contact:** Must be changed to another user before removal
- **Points of Contact:** Remove from all billing contact roles
- **Billing notifications:** Ensure another admin receives account alerts
- **Super admin privileges:** Transfer or revoke super admin access immediately

Critical: You cannot remove a user who is set as Primary Account Contact—reassign this role first.

Security Priority: Administrative accounts have elevated privileges that can compromise the entire HubSpot environment. Prioritize removal of former admins within 24 hours of departure.

6. Content and Social Media

- **Social accounts:** If the user was an admin, reconnect accounts under another user
- **Blog author:** User remains as author—manually delete author profile if needed
- **Marketing emails:** Creator information disappears—document ownership before removal
- **Templates:** Ensure sales templates are shared before removal
- **Documents:** Verify shared documents remain accessible
- **Connected accounts:** Audit all OAuth connections and social media integrations for removal

Security Note: Connected social media accounts can provide access to broader corporate social presence. Audit and revoke all connected services immediately.

Step by step Secure Removal Process

Access Control Security Best Practices Framework admindroid.com

Phase 1: Immediate Security Actions (Within 2 Hours)

1. Identify user departure and notify IT/Security team
2. Immediately deactivate the user to prevent access
3. Revoke API keys and access tokens
4. Disable scheduling pages and external-facing links
5. Reset passwords on any shared accounts
6. Review recent user activity for anomalies

Security Rationale: The window between employee notification and access revocation is the highest risk period. Disgruntled employees or compromised accounts can exltrate data, create backdoors, or modify critical configurations.

Phase 2: Comprehensive Audit (Hours 3-24)

1. Export complete list of owned records (contacts, companies,deals, tickets)
2. Document workflow and automation involvement
3. Map all permission sets and custom roles
4. Identify integration connections and API usage
5. Review audit logs for recent activity
6. Check for any automated email sending or sequences

Phase 3: Asset Reassignment (Hours 24-72)

1. Bulk reassign all owned records to designated owner(s)
2. Use find/replace in workflows to update user references
3. Remove from rotation owners and sequences
4. Transfer or disable scheduling pages
5. Update meeting rotations
6. Remove paid seats

Phase 4: Verification and Testing (Hours 48-72)

1. Confirm user cannot log in
2. Test workflows still function correctly
3. Verify new leads route to active users
4. Check reports display historical data correctly
5. Monitor for any assignment gaps

Phase 5: Complete Removal (72 Hours After Deactivation)

1. Navigate to Settings → Users & Teams
2. Filter by "Deactivated" status
3. Click user name → Actions → Remove from account
4. Review the final advisory and confirm no operational gaps
5. Click Continue → Confirm permanent removal
6. Document removal in the security audit log
7. Verify the user profile no longer appears in the system

Security Recommendation: Complete removal within 72 hours of deactivation. Extended deactivation periods maintain unnecessary attack surface. The 72-hour window allows for verification and asset transition while minimizing security exposure.

Compliance Note: Maintain documentation of user removal for audit and compliance purposes. Record: removal date, assigned assets disposition, and authorizing personnel.

Special Considerations for FrontierZero Customers

Sales and Revenue Team Members

- Prioritize deal reassignment—open deals must transfer immediately
- Update sales forecast ownership to reflect new territory assignments
- Update lead assignment workflows for web leads
- Check sequence enrollment for scheduled follow-ups
- Review the quote and proposal access permissions
- Audit pricing and discount approval authorities

Security Note: Sales team members often have access to sensitive pricing, strategic accounts, and competitive intelligence. Prioritize complete removal to prevent potential data exfiltration to competitors.

Partnership and Channel Team Members

- Review partner contact ownership and NDA obligations
- Transfer active partnership deals and opportunities
- Update any partner-specific workflows
- Reassign partnership tasks and follow-ups
- Audit access to partner portals and shared resources
- Revoke channel partner system access

Security Note: Partnership team members frequently have credentials for external partner systems. Coordinate with partners to revoke access to shared platforms and partner portals.

Administrative and Super Admin Users

- Change Primary Account Contact before removal (mandatory)
- Update billing notification recipients
- Transfer super admin permissions immediately
- Review system-level workflow ownership
- Audit integration admin rights (Salesforce, Slack, etc.)
- Review data export and API access history
- Force a password reset on all admin accounts as a precaution

Critical Security Priority: Administrative accounts represent the highest risk. Former admins retain knowledge of system architecture, integration points, and security configurations. Complete removal within 24 hours is mandatory. Consider this a P0 security incident requiring immediate action.

Common Security And Operational Pitfalls

1. **Removing before deactivating:** HubSpot requires deactivation first—the system will block the operation
2. **Delayed deactivation:** Waiting until "a convenient time" increases security exposure—deactivate immediately
3. **Skipping workflow updates:** Automated processes break if the user is referenced in the criteria
4. **Forgetting rotation owners:** Deactivated users are skipped in rotations—leads may be dropped
5. **Not revoking API access:** Personal API keys remain active even after deactivation
6. **Removing Primary Account Contact:** System blocks removal— must reassign role rst
7. **Extended deactivation periods:** Keeping accounts deactivated for months maintains the attack surface unnecessarily
8. **Ignoring connected services:** OAuth tokens and integration often persist after deactivation
9. **No audit trail:** Failing to document removal creates compliance gaps
10. **Forgotten shared credentials:** User may have shared passwords for team accounts that need rotation

Quick Reference Security Decision Framework

User Departure Security Protocol

- **Has the user departed or been terminated**
  - Yes - Deactivate immediately (within 2 hours)
  - No - Proceed with standard offboarding timeline

- **Is this an administrative or privileged account?**
  - Yes - Complete removal within 24 hours (P0 priority)
  - No - Standard 72-hour removal timeline

- **All assets reassigned and workflows updated?**
  - Yes - Proceed to complete removal immediately
  - No - Complete reassignment within 48 hours while the account remains deactivated

- **Are there connected external systems or APIs?**
  - Yes - Revoke all API keys and OAuth tokens before removal
  - No - Proceed to removal

Recommended Security First Workflow

Security optimized timeline for user removal (Standard accounts)

Timeline	Action	Owner	Priority	Status
0-2 hours	Immediate deactivation	Super Admin	P0	☐
0-2 hours	Revoke API keys and tokens	Admin	P0	☐
0-2 hours	Disable external scheduling links	Admin	P1	☐
3-24 hours	Comprehensive audit and asset mapping	Admin	P1	☐
24-48 hours	Reassign records and update workflows	Admin + Team Lead	P1	☐
24-48 hours	Remove paid seats	Admin	P2	☐
48-72 hours	Verify system functionality	Admin	P2	☐
72 hours	Complete permanent removal	Super Admin	P1	☐
72+ hours	Document in security audit log	Security Team	P2	☐

Security optimized timeline for administrative/privileged accounts

Timeline	Action	Owner	Priority	Status
0-1 hours	Immediate deactivation	Super Admin	P0	☐
0-1 hours	Revoke API keys and tokens	Super Admin	P0	☐
1-4 hours	Disable external scheduling links	Security Team	P0	☐
4-12 hours	Comprehensive audit and asset mapping	Admin + Leadership	P0	☐
12-24 hours	Reassign records and update workflows	Super Admin	P0	☐
24+hours	Remove paid seats	Security Team	P1	☐

Key Security Takeaways

1. **Default to complete removal** rather than extended deactivation—every inactive account is a security liability
2. **Deactivate immediately upon departure**—within 2 hours for standard accounts, within 1 hour for administrative accounts
3. **72-hour removal window**—sufficient time to reassign assets while minimizing security exposure
4. **Prioritize administrative accounts**—former admins representthe highest risk and require 24-hour removal
5. **Always revoke API access**—personal API keys remain active after deactivation and must be explicitly revoked
6. **Reassign assets during the deactivation period**—records, workflows, rotations, and meetings must transfer to active users
7. **Use HubSpot's find/replace tool** for workflows to efficiently update user references system-wide
8. **Never remove Primary Account Contact** without reassigning the role first—system will block the operation
9. **Document everything**—maintain an audit trail of user removals for compliance and security reviews
10. **Coordinate with external systems**—revoke access to partner portals, integrations, and connected services

Security Principles Behind this Guidance

Principle of Least Privilege
Every user should have only the minimum access necessary to perform their job. When that job ends, all access must be revoked immediately.

Zero Trust Architecture
Never assume inactive accounts are secure. Treat every deactivatedaccount as a potential vulnerability until completely removed.

Attack Surface Reduction
Each inactive account represents a potential entry point for threat actors. Reducing the number of accounts reduces the attack surface proportionally.

Defense in Depth
User removal is one layer in a comprehensive security strategy. Combine with strong password policies, MFA enforcement, and regular access reviews.

About FrontierZero

FrontierZero is a cybersecurity AI company specializing in third-party risk management and attack surface reduction across modern SaaS environments. This guide reflects our security-first philosophy: every access point is a potential vulnerability, and proactive removal of unnecessary accounts is a fundamental security control.

Our Approach: We help organizations minimize their attack surface through automated risk assessment, continuous monitoring, and security-first operational practices. User access management is a critical component of a comprehensive cybersecurity posture.

Modern organizations operate across dozens or even hundreds of SaaS platforms. Security teams often have strong visibility inside core systems like Microsoft or Google, but much of the real risk lives across the broader SaaS ecosystem — third-party tools, integrations, external users, and shadow applications.

At FrontierZero, we provide a single pane of glass across the entire SaaS landscape, using Pattern-of-Life analysis to detect anomalies such as unusual login locations, dormant accounts becoming active again, or unexpected third-party access.

Because in modern breaches, attackers rarely break in. They log in.

FrontierZero helps organizations detect these risks early, reduce unnecessary access, and continuously monitor identity activity across their SaaS ecosystem.

Explore more security guides at FrontierZero.io