Security & Risk Assessment

COA Discord Staff-Only Collaboration Server

Prepared by: DJ Broadbent, SUNY Potsdam | SUNY COA Executive Council
Date: June 2026 (Reviewed & approved for this use case by SUNY System Administration ISO)

1. Executive Summary

This assessment evaluates the security posture and risk profile of a staff-only Discord server established by the SUNY Computing Officers Association (COA) for internal collaboration among SUNY IT professionals. The server utilizes SUNY-federated authentication and is restricted exclusively to verified SUNY staff.

Overall Risk Rating: LOW — The combination of strict access controls, federated identity management, absence of sensitive institutional or student data, and robust platform-level security features results in a low residual risk profile suitable for internal professional collaboration.

2. Purpose and Background

The SUNY Computing Officers Association (COA) is a long-standing community of practice comprising IT professionals across all 64 SUNY campuses. In early 2026, COA launched a dedicated Discord server to facilitate real-time collaboration, knowledge sharing, and community building among staff.

Several campuses have requested formal security guidance before broader adoption. This assessment addresses those concerns and provides a referenceable framework aligned with SUNY Information Security Policy 6900, which requires institutions to assess and manage risks associated with third-party vendors processing institutional information.

3. Scope and Use Case

3.1 Intended Use

- Internal staff collaboration and knowledge sharing among SUNY IT professionals
- Discussion of technical topics, best practices, and professional development
- Event coordination and community building within COA
- No student data, Protected Health Information (PHI), financial data, or other sensitive institutional records will be stored or discussed

3.2 Access Model

The server is configured as staff-only. Users join via standard Discord invite. The public "@everyone" role has limited access only to a few public informational channels. Those channels direct users to the COA-controlled authentication portal at https://discauth.org/suny.
The portal (developed and maintained by COA) logs every login and every interaction with Discord. Users authenticate via Discord OAuth + SUNY Federated SAML. Upon successful authentication, the portal assigns the "Verified" role (required for privileged channels), the "COA" role (for most collaboration channels), specialized roles as applicable (e.g. Executive Council, Collaboration Leader), and "SUNY verified" metadata. Privileged channels are restricted to users holding the "Verified" role.

4. Technical Implementation

Authentication: SUNY Federated Login (SAML/OIDC via discauth.org) — provides strong identity assurance and automatic revocation upon separation from SUNY employment.

Server Type: Private Discord Server with Community features enabled (rules screening, verification levels, welcome screen).

Administrative Control: COA Executive Council maintains full server ownership and moderation privileges, including role-based access control, channel permissions, and content moderation settings.

5. Security Controls and Mitigations

5.1 Platform-Level Security (Discord)

Discord maintains a formal Information Security Program (updated January 2026) covering:

- Access control, vulnerability management, incident response, and malware protection
- Physical and logical security controls at processing locations
- Personnel security awareness training and background screening
- Data classification and secure data handling procedures
- Transport Layer Security (TLS) for data in transit; DAVE end-to-end encryption for voice/video calls (rolled out March 2026)

5.2 Server-Level Controls (COA Implementation)

- **Strict Access Control:** Federated SSO + manual approval workflow; no public invites or guest access
- **Role-Based Permissions:** Granular channel visibility and posting rights based on COA roles
- **Content Moderation:** AutoMod enabled for profanity, spam, and sensitive content; explicit community guidelines with rules screening
- **Account Security:** All members encouraged/required to enable MFA; server verification level set to "High"
- **Audit & Monitoring:** Regular review of member list, audit logs, and moderation actions by COA leadership
- **Data Minimization:** No persistent storage of sensitive files; ephemeral voice channels preferred for sensitive discussions

6. Risk Assessment

A qualitative risk assessment was performed considering likelihood and impact across key threat categories:

Risk Category	Likelihood	Impact	Mitigation & Residual Risk
Unauthorized Access	Low	Medium	Federated SSO + manual approval; residual risk LOW
Data Exposure / Leak	Low	Low	No sensitive data stored; text not E2EE but low sensitivity; residual LOW
Malicious Content / Phishing	Medium	Low	AutoMod + rules screening + staff-only audience; residual LOW
Account Compromise	Low	Medium	MFA encouraged; federated auth reduces impact; residual LOW

Regulatory / Compliance	Low	Low	No PHI/FERPA data; internal use only; residual LOW

Conclusion: All identified risks are rated LOW after mitigation. The server presents a low-risk profile appropriate for its intended internal professional use.

7. Compliance and Regulatory Considerations

SUNY Policy 6900 (Information Security Policy): This assessment fulfills the vendor risk management requirements outlined in Section 4.4. The server processes only low-sensitivity collaboration data among authorized staff.

FERPA / HIPAA / PCI: Not applicable. No student education records, protected health information, or payment card data will be processed or stored on the server.

Data Residency & Sovereignty: Discord operates primarily in the United States. All data remains within Discord's infrastructure; no cross-border transfer concerns for this internal use case.

8. Recommendations

1. **Approve for Use:** Grant formal acknowledgment that the COA Discord server meets SUNY security expectations for internal staff collaboration.
2. **Publish Guidance:** Share this assessment (or a summary) with campus ISOs to support informed adoption decisions.
3. **Ongoing Monitoring:** COA commits to quarterly security reviews and immediate reporting of any incidents to System Administration.
4. **Future Enhancements:** Explore Discord's enterprise features (if made available) or complementary tools as needs evolve.

9. Conclusion

The COA Discord staff-only server represents a low-risk, high-value collaboration tool that strengthens the SUNY IT community of practice. With strong access controls (federated SSO via the custom discauth portal), platform security features, and clear operational boundaries, it aligns well with SUNY's information security objectives for this specific use case.

This assessment has been reviewed and approved for the specific use case of the restricted, staff-only COA Discord server (authenticated via SUNY Federated SSO) by an Information Security Officer from SUNY System Administration. COA is now positioned to distribute this document and promote the server for broader staff adoption.

Please contact DJ Broadbent (broadbdj@potsdam.edu) with any questions.

Submitted by,

DJ Broadbent
SUNY Potsdam | SUNY COA Executive Council
broadbdj@potsdam.edu

10. FAQ: Common Campus ISO Questions & Responses

Q: What events are captured in Discord's server audit logs, and how long are they retained?
A: Discord's audit logs record administrative actions such as role/permission changes, member kicks/bans, channel modifications, and bot activities. They are visible in Server Settings (to users with the View Audit Log permission) and accessible via the API. Retention is approximately 45 days. We recommend campuses supplement this with their own SSO logs for longer-term auditing. See: https://docs.discord.com/developers/resources/audit-log

Q: How is deprovisioning handled when a staff member leaves SUNY?
A: When a user's SUNY account is disabled or revoked through the federated identity provider, the linked Discord access should be invalidated. The discauth portal and COA admins can also manually remove roles or ban the account if needed. This provides a reliable offboarding process similar to other SSO-integrated tools.

Q: What about data retention, encryption, and potential FERPA concerns?
A: Messages, files, and logs follow Discord's standard retention policies. Encryption is used in transit (TLS). There is no end-to-end encryption for standard text messages/channels. Voice and video calls support end-to-end encryption via Discord's DAVE protocol (see https://discord.com/blog/meet-dave-e2ee-for-audio-video). At-rest protection is handled by Discord's infrastructure. As with Teams or GitHub, the primary control against sensitive data exposure is user education. Discord publishes transparency reports on enforcement and data requests. See: https://discord.com/safety-transparency and https://discord.com/privacy

Q: Who owns and administers the server?
A: The SUNY COA owns and operates the server. Primary administrators are DJ Broadbent and Dan Laird (both members of the COA Executive Committee). All moderation follows COA guidelines, with clear escalation paths to campus security teams if needed.

Q: How does the risk profile compare to other approved tools?
A: The risk is comparable to (or lower than) enterprise GitHub with SSO, Microsoft Teams guest access, or Slack workspaces. There is no additional cost to campuses, and it runs in parallel with existing tools. Discord is used by many large technical organizations (including Microsoft support communities).

Q: How are security incidents or compromised accounts handled?
A: Discord provides strong real-time protections (AutoMod, raid/CAPTCHA protection, spam filtering, and 2FA enforcement for moderator actions). For a post-authentication compromise, COA admins can quickly revoke roles or ban the account. Incidents would be escalated following standard SUNY procedures and cross-referenced with campus SSO logs.