ADMINISTRATIVE PROCEDURES AND GUIDELINES

CYBERSECURITY AND DATA PROTECTION CONTROLS

Approved | Version 1.0 | Prepared By Yolanda Butler | November 6, 2026 | Effective November 9, 2026

Purpose And Scope

Keep GFMN's data safe while people get their work done. Use one request and one linked approval record. Keep controls clear, suited to the risk and easy to follow, without duplicate forms or extra approval steps for work already authorized.

These guidelines apply to all directors, officers, employees, contractors, subcontractors, interns and volunteers doing GFMN work, including remote work. They cover registrations, systems access, information handling and mandatory training.

Roles And Approval Authority

Only the designated Cybersecurity and Data Protection Officer (CDPO), Secretary or Executive Director (ED), as required, may approve registrations that involve sensitive, confidential or restricted systems or data, or the use or sharing of restricted GFMN information.

Routine work within a recorded standing approval can continue. Return changes in recipient, purpose, records or conditions to an authorized approver. Record the approver, decision and permitted scope once.

Role	What the role does here
Cybersecurity and Data Protection Officer (CDPO)	Leads security and data protection; approves registrations, access, use and sharing under this procedure.
Secretary	Reviews and approves requests when required; keeps the approval record.
Executive Director (ED)	Reviews and approves requests when required; coordinates implementation.

Requesting Registration Or Access

1. Describe the need. Complete Part 1 of Addendum A, or an equivalent written request, and send it to an authorized approver. Include the platform, purpose, requested records, deadline, fee and any existing approval reference.

2. Get the required approval. The approver checks the recipient, purpose, minimum records needed, access and secure method. Complete Part 2, or link an equivalent written decision, before granting access or sharing data. Identify the approver, decision, permitted scope and conditions; cite an existing approval when it applies.

3. Check spending requirements. Fees and commitments follow the Decision Matrix and adopted financial controls. Observe any spending pause.

4. Complete and record. Submit securely, keep the approval and confirmation together, notify the requester and complete Part 3 or an equivalent linked record. Refer scope changes to an authorized approver.

Everyday Data Protection

Collect, use and share only the data needed for authorized work. Check recipients; use approved storage, secure transfers, access based on assigned roles, unique credentials, multifactor authentication (MFA) where supported and current device updates. Follow retention, disposal and legal-hold requirements. Report suspected phishing, lost devices or unauthorized access or sharing to the CDPO immediately.

Laws And Other Obligations

The CDPO leads cybersecurity, privacy and breach-notification compliance. The ED coordinates employment, grant and contract obligations. Apply the requirements relevant to GFMN's activities and data, and obtain qualified guidance when needed.

Official references (reviewed November 7, 2026): Minn. Stat. 325E.61 - breach notification; CISA - security awareness; EEOC - harassment prevention practices.

Annual Training

All directors, officers, employees, contractors, subcontractors, interns and volunteers doing GFMN work must complete all four subjects at onboarding and at least once every 12 months. Training must fit their roles. The annual cycle is a GFMN requirement; any additional legal or contractual requirements also apply.

Training subject	What it covers
Cybersecurity	Phishing and fraud; safe use of accounts and devices; strong passwords, MFA and prompt incident reporting.
Data protection	Confidentiality, only the data needed, approved access and sharing, retention, secure disposal and applicable privacy duties.
Anti-harassment	Prohibited conduct, practical examples, accessible reporting routes, protection from retaliation and managers' response duties.
Code of Business Conduct and Professional Ethics	GFMN's current Code, conflicts of interest, professional boundaries, responsible use of resources and reporting concerns.

Delivery And Completion Records

The CDPO coordinates accessible training and completion dates. Use practical examples and allow questions. Combined modules or verified equivalent courses may cover the four subjects without duplication. Employees receive paid time as required by law; respect applicable agreements.

Keep one restricted completion register with name, role, subjects, provider, completion date, next due date and acknowledgment. Address overdue training through existing accountability procedures.

Publish security and complaint contacts, including an independent route for concerns involving the usual contact. Report completion rates and material gaps to the ED without unnecessary personal details.

Addendum A: Registration Request And Authorization

One record covers the request, approval and completion. Authorized approvers are the designated CDPO, Secretary or ED, as required. Use supporting records for longer details.

Part 1 Request

Requester name

Requester email or phone

Organization or platform

Registration URL or contact

Purpose of registration and intended use

Records or data requested - names only

Needed by

Fee amount and recurrence - Free or Unknown if applicable

Existing approval reference, if any

Part 2 Approval By An Authorized Approver

Approver name

Decision date

Approver role - select one

Select a role

Decision - select one

Select a decision

Approved scope, conditions or reason

Written approval reference

Part 3 Completion

Completed by and date; confirmation reference; requester notification date

Keep sensitive contents off this form: no actual EINs, banking details, passwords or confidential records. Store supporting records securely. A request alone is not approval.