



OFFICIAL ELEMENT ESPORTS POLICY

INFORMATION SECURITY AND RECORDS POLICY

DOCUMENT CODE	OPS-POL-001
VERSION	1.0
EFFECTIVE DATE	OCTOBER 4, 2026
POLICY OWNER	ELEMENT ESPORTS LEADERSHIP

Element Esports is the non-FPS sister organization of ADHD Esports. This edition preserves the shared leadership and operating standard while applying Element branding, contacts, community structure, and game scope.

Role terminology: formal position names govern authority and responsibility. Element-themed names are friendly Discord display roles only unless a written appointment states otherwise.

OFFICIAL ORGANIZATIONAL POLICY

INFORMATION SECURITY & RECORDS POLICY Least privilege, account protection, data minimization, confidential records, incident response, continuity, and secure offboarding.

DOCUMENT CODE VERSION EFFECTIVE OWNER OPS-POL-001 1.0 AUG 27, 2026 Technology & Systems

CONTROL NOTICE This PDF is the controlled distribution version. The accessible web reading version is at adhdesports.joshdisciple.chatgpt.site/policies/information-security-records. If a later version is posted there, the later approved version controls. This policy is organizational guidance, not legal advice.

DOCUMENT CONTENTS - 1. Purpose and security principles - 9. Records and retention - 2. Scope and assets - 10. Backups and continuity - 3. Information classes - 11. Security incident response - 4. Account ownership - 12. Offboarding and role change - 5. Authentication - 13. Prohibited activity - 6. Access lifecycle - Implementation checklist - 7. Handling and sharing - Shared administration - 8. Devices and remote work - Cross-references and source notes

Effective August 27, 2026 | Version 1.0 Official web version: adhdesports.joshdisciple.chatgpt.site/policies

1. Purpose and security principles Element Esports protects information and systems according to sensitivity, operational importance, and realistic risk. Access is granted because a role needs it, not as status. Minimum principles are least privilege, unique identity, multifactor authentication, data minimization, recoverability, prompt reporting, and documented ownership.

2. Scope and assets Covered assets include organizational email, Discord, social media, Sites, domains, cloud drives, tournament systems, game accounts, code, automation, credentials, applications, minor and guardian information, reports, agreements, finances, partner records, strategies, rosters, creative source files, devices, backups, and exports.

3. Information classes

Public: approved for unrestricted release.

Internal: routine organizational information not intended for public release.

Confidential: applicant, member, partner, competitive, financial, agreement, source, or operational information requiring limited access.

Restricted: credentials, recovery data, minors and guardians, safeguarding, incident, discipline, health, identity, payment, security, or legally protected records requiring the narrowest access.

4. Account ownership Critical accounts should be organization-controlled, have a named business owner and technical custodian, use current recovery information, and avoid dependence on one person's private account. Shared generic logins are minimized; where unavoidable, use an approved password manager and auditable access process.

5. Authentication

Use unique strong passwords and never reuse organizational credentials on personal services.

Enable multifactor authentication on email, social, financial, hosting, domain, storage, and administrator accounts; prefer phishing-resistant methods where available.

Protect recovery codes and do not send passwords or secrets through ordinary chat.

Report unexpected prompts, login alerts, password-reset messages, phishing, SIM changes, or suspicious sessions immediately.

6. Access lifecycle A lead requests access tied to defined duties; a system owner approves the minimum role; the custodian records and grants it; the lead reviews it after role change, inactivity, elevated work, or at least periodically. Elevated access must be removed promptly when no longer needed.

7. Handling and sharing Use approved channels, verify recipients, restrict link permissions, avoid unnecessary exports, and store source records where authorized people can recover them. Do not place restricted information in public channels, personal AI tools, unapproved forms, public links, screenshots, or personal devices without a defined need and protection.

Effective August 27, 2026 | Version 1.0 Official web version: adhdports.joshdiscipline.chatgpt.site/policies

8. Devices and remote work Keep supported software current, use screen locks, protect devices from household or public access, avoid unknown software and browser extensions, and separate organizational work where practical. Lost, stolen, infected, or shared devices with organizational access must be reported promptly.

9. Records and retention The record owner identifies purpose, sensitivity, source of truth, authorized access, retention target, and disposal method. Incident, governance, agreement, finance, prize, partner, and major decision records are retained long enough for accountability and applicable obligations. Duplicate personal copies and obsolete exports should be deleted securely.

10. Backups and continuity Critical websites, brand masters, agreements, policy records, account inventories, and operational documentation require recoverable copies or platform version history. At least two authorized people should be able to recover critical services without sharing personal credentials.

11. Security incident response

Report and preserve evidence without public speculation.

Contain affected sessions, credentials, links, devices, and permissions through authorized action.

Assess affected people, data, systems, availability, minors, finances, and legal notice duties.

Recover from verified ownership and trusted backups; monitor for recurrence.

Record the incident, response, unresolved risk, notification, and preventive changes.

12. Offboarding and role change Remove accounts and groups, rotate exposed shared secrets, transfer files and ownership, recover equipment, preserve required records, revoke tokens and integrations, update contact and recovery data, and confirm completion. Separation does not authorize deletion of organizational records or retention of restricted copies.

13. Prohibited activity

Unauthorized monitoring, scraping, impersonation, access testing, privilege escalation, credential use, or data export.

Using organizational information for harassment, retaliation, competition against the organization, personal commerce, or leverage.

Disabling logs, backups, security controls, or administrator access without approval.

Concealing compromise, deleting evidence, or privately negotiating with an attacker.

Effective August 27, 2026 | Version 1.0 Official web version: adhdports.joshdiscipline.chatgpt.site/policies

IMPLEMENTATION CHECKLIST The responsible policy owner should use this checklist to turn the written standard into routine practice.

1 Inventory critical accounts, owners, custodians, recovery methods, and MFA status. 2 Review administrator and high-risk permissions at least quarterly. 3 Define retention targets for applications, incidents, agreements, finance, and minor records. 4 Maintain an offboarding checklist and tested recovery path. 5 Run a phishing and account-compromise tabletop exercise annually.

SHARED ADMINISTRATION Policy status and relationship This is an official Element Esports organizational policy. It supplements the Staff & Player Handbook and does not create employment, collective-bargaining, public-sector, or union rights. A completed agreement, applicable law, platform or tournament rule, or stricter safety requirement may add

obligations.

When policies overlap, the most protective applicable safeguarding or safety rule controls immediate action. Findings, corrective action, and appeals use the Discipline & Appeals Policy unless a specific external authority controls.

Administration and interpretation Ownership retains ultimate policy authority. The named policy owner administers day-to-day implementation, may issue consistent procedures and forms, and must elevate material ambiguity, conflicts, or requested exceptions.

Exceptions must be written, limited, lawful, time-bounded when appropriate, and may not waive safeguarding, non-retaliation, fair-play, privacy, or truthful-advertising requirements.

Reporting and non-retaliation Good-faith questions, disclosures, mistakes, and concerns may be raised to a direct lead, department head, Management, Ownership, or the Report a Concern route. A person may bypass the chain when it is unsafe, unavailable, or conflicted.

Retaliation, evidence destruction, witness pressure, coordinated stories, restriction evasion, or misuse of authority to suppress reporting are separate potential violations. An unsubstantiated report is not automatically false or malicious.

Review, records, and appeals Material decisions should identify the issue, governing standard, relevant information, conflicts, action, responsible owner, duration or review date, and required notice. Access to reports and records is limited to legitimate need.

Protective restrictions may be imposed before a finding when safety, minors, accounts, evidence, competition, finances, or operations are reasonably at risk. Formal outcomes and material restrictions may be appealed under Discipline & Appeals.

Training, acknowledgment, and review People with elevated authority or access must receive role-appropriate instruction and acknowledge this policy before or soon after assignment. Leadership should review the policy after a material incident, program change, legal or platform development, or at least annually.

CROSS-REFERENCES

Staff & Player Handbook

Staff & Member Conduct Policy

Discipline & Appeals Policy

Effective August 27, 2026 | Version 1.0 Official web version: adhesports.joshdisciple.chatgpt.site/policies

Community Standards

Safeguarding and Minor Participation Policies

Privacy Policy

Brand Guidelines

Applicable role agreement, tournament, platform, publisher, partner, and legal requirements

SOURCE NOTES These sources informed the policy's general prevention, disclosure, security, or rights principles. They do not determine whether employment law or another law applies to a particular volunteer relationship.

CISA, More than a Password: <https://www.cisa.gov/MFA>

CISA, Require Multifactor Authentication:

<https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication>

DOCUMENT Owner / authorized representative: _____ APPROVAL

VERSION CONTROL Approved date: _____ Next review: _____

Effective August 27, 2026 | Version 1.0 Official web version: adhdports.joshdisciple.chatgpt.site/policies

Questions, reports, and requests for the current controlled copy: contact@elementesports.com