

**6005 - CYBERSECURITY INCIDENT RESPONSE, DATA BREACH,
BUSINESS CONTINUITY AND RECOVERY POLICY**

ODYSSEY CHARTER SCHOOL, INC.

1. PURPOSE

Odyssey Charter School, Inc. (“Odyssey”) recognizes its responsibility to protect the confidentiality, integrity, and availability of student, employee, financial, operational, and other sensitive information and to maintain essential school operations during and following a cybersecurity incident.

The purpose of this policy is to establish the framework for prevention, identification, containment, investigation, notification, recovery, and review of cybersecurity incidents and data breaches affecting Odyssey.

2. SCOPE

This policy applies to all schools, programs, employees, Board members, systems, networks, devices, applications, data, and technology resources operated by or on behalf of Odyssey.

The policy also applies, as appropriate, to contractors, consultants, management/support providers, technology vendors, cloud providers, and other third parties that access, maintain, store, process, or transmit Odyssey information.

3. PROTECTION OF INFORMATION AND SYSTEMS

Odyssey shall take reasonable administrative, technical, and physical measures to protect its information systems and confidential information.

Such measures may include, as appropriate:

- Access controls and multifactor authentication;
- Endpoint protection and monitoring;
- Network security and segmentation;
- Security updates and patch management;
- Secure backups and recovery capabilities;
- Employee cybersecurity training;
- Appropriate password and credential practices;
- Vendor security requirements; and
- Periodic review and testing of security and recovery procedures.

4. REPORTING CYBERSECURITY INCIDENTS

Employees and contractors shall immediately report suspected or known cybersecurity incidents, including unusual computer activity, ransomware, malware, unauthorized access, compromised credentials, loss of sensitive information, or other suspected security events, in accordance with established administrative procedures.

Employees shall not independently investigate, communicate with a suspected threat actor, delete potentially relevant information, or take other action that could compromise evidence unless directed by authorized personnel.

5. CYBERSECURITY INCIDENT RESPONSE AND RECOVERY PLAN

Upon discovery of a suspected cybersecurity incident, Administration (the School Leader or other administrator designated by the Governing Board, or such individual’s authorized designee) shall promptly initiate Odyssey’s Incident Response and Recovery Plan.

Depending upon the circumstances, actions may include:

1. Isolating or disconnecting affected systems or devices;

2. Preserving relevant logs, records, equipment, and other evidence;
3. Engaging or notifying, as appropriate, cybersecurity, forensic, legal, cyber-insurance, law-enforcement, communications, and technology professionals;
4. Protecting unaffected systems from further compromise;
5. Resetting or securing credentials where appropriate;
6. Determining the scope and nature of the incident;
7. Determining whether data was accessed, acquired, altered, encrypted, destroyed, or exfiltrated;
8. Coordinating with law enforcement or governmental agencies when appropriate; and
9. Maintaining documentation of significant response and recovery actions.

Protection of students, employees, sensitive information, and essential school operations shall be prioritized.

6. DATA BREACH ASSESSMENT AND NOTIFICATION

Odyssey shall promptly investigate suspected unauthorized access to personal or confidential information and, as appropriate, coordinate the investigation through legal counsel and qualified cybersecurity professionals. Odyssey shall determine whether the event constitutes a reportable breach and what investigation, documentation, reporting, notification, remediation, or other action is required under applicable law. Odyssey shall comply with any applicable reporting obligations owed to its charter school sponsor, insurers, law-enforcement agencies, governmental entities, and contracting parties.

When notification is legally required, Odyssey shall provide it as expeditiously as practicable and without unreasonable delay, and no later than the deadline established by applicable law, subject to any legally authorized delay, extension, or waiver.

For purposes of Florida's data breach requirements, Odyssey shall comply, as applicable, with section 501.171, Florida Statutes, including requirements concerning notification to affected individuals, the Florida Department of Legal Affairs, and other required entities.

Third-party providers that maintain, process, or store Odyssey information shall be required to notify Odyssey of a suspected or confirmed breach as expeditiously as practicable and within any period required by applicable law or contract, and shall provide timely and continuing cooperation and information necessary for Odyssey to satisfy its legal, contractual, insurance, investigative, and notification responsibilities.

7. STUDENT AND EMPLOYEE INFORMATION

Student education records shall be protected consistent with the Family Educational Rights and Privacy Act (FERPA), sections 1002.22 and 1002.221, Florida Statutes, and other applicable laws.

Employee records, financial information, identification information, medical information, credentials, and other confidential or exempt information shall be protected in accordance with applicable federal and Florida law.

8. BUSINESS CONTINUITY

Odyssey shall maintain procedures designed to continue essential educational and business operations when technology systems are unavailable.

Continuity procedures shall address, as appropriate, essential functions including:

- Student safety and communications;
- Enrollment and student information;
- Attendance and state reporting;
- Instruction and assessment;
- Transportation;
- Food and nutrition services;
- VPK and before/after care programs;
- Human resources and payroll;

- Finance and purchasing; and
- Other time-sensitive state, federal, district, or contractual requirements.

Temporary manual or alternative procedures may be used when necessary to maintain operations while technology systems are restored.

9. SYSTEM RECOVERY AND RESTORATION

Restoration following a cybersecurity incident shall be deliberate and controlled. Systems shall not be returned to normal operation solely because they are technically capable of being restarted. Administration, in coordination with cybersecurity and technology professionals, shall determine when affected systems are sufficiently secure for restoration.

Recovery procedures shall address, as applicable:

1. Identification and removal or containment of the threat;
2. Verification of clean and reliable backups;
3. Remediation of identified vulnerabilities;
4. Installation or verification of security monitoring and endpoint protection;
5. Credential resets or access changes when warranted;
6. Testing of restored systems;
7. Validation of data integrity;
8. Prioritization of critical operational systems; and
9. Monitoring of restored systems for indications of continuing or renewed compromise.

Restoration shall be prioritized based upon student safety, legal and regulatory deadlines, instructional needs, and operational importance.

10. INCIDENT RESPONSE AND RECOVERY PLAN

Administration shall maintain a separate Cybersecurity Incident Response and Recovery Plan establishing detailed procedures for carrying out this policy.

The Plan may include:

- Cyber-insurance notice, consent, and vendor-authorization requirements;
- Sponsor, governmental, and contractual reporting requirements;
- Decision-making authority for system isolation, shutdown, restoration, and public communications;
- Procedures for recording legally required determinations, notices, delays, and disclosure records;
- Procedures for documenting unauthorized access to or disclosure of student education records, including any disclosure records required by applicable law;
- Incident-response roles and responsibilities;
- Emergency contact information;
- Cybersecurity and forensic providers;
- Legal counsel and cyber-insurance contacts;
- Law-enforcement and governmental contacts;
- System inventories and restoration priorities;
- Backup and recovery procedures;
- Communication protocols;
- Evidence-preservation procedures;
- Vendor responsibilities;
- Alternative operating procedures; and
- System-specific restoration requirements

Security-sensitive portions of the Plan and related cybersecurity records shall be maintained, handled, and disclosed in accordance with applicable law. Information made confidential and exempt from public disclosure shall be appropriately identified, segregated, and protected. Nothing in this policy authorizes withholding a record or closing any portion of a meeting except as expressly permitted by law.

11. THIRD-PARTY SERVICE PROVIDERS

Contracts involving access to or storage of confidential Odyssey information shall contain, to the extent appropriate for the nature and risk of the services, data-security provisions, including requirements relating to:

- Protection of confidential information;
- Access controls;
- Cybersecurity safeguards;
- Incident and breach notification;
- Cooperation with forensic investigations;
- Preservation of relevant evidence;
- Return or secure destruction of information when appropriate; and
- Compliance with applicable privacy and security laws.

12. COMMUNICATIONS

Information concerning an active cybersecurity incident shall be communicated only through individuals authorized by Administration in consultation with legal counsel and cybersecurity professionals.

Communications shall be accurate and timely while avoiding disclosure of information that could compromise an investigation, expose security vulnerabilities, interfere with law enforcement, or violate privacy requirements.

13. DOCUMENTATION AND RECORDS

Odyssey shall maintain appropriate records relating to cybersecurity incidents, including actions taken to contain, investigate, remediate, recover from, and evaluate an incident.

Records shall be maintained and protected in accordance with applicable record-retention, confidentiality, public-records, student-records, attorney-client privilege, and work-product requirements.

14. POST-INCIDENT REVIEW

Following a significant cybersecurity incident, Administration shall conduct or obtain an after-action review addressing, as appropriate:

- The nature and cause of the incident;
- Effectiveness of the response;
- Systems and information affected;
- Effectiveness of backups and recovery procedures;
- Operational disruptions;
- Security improvements;
- Vendor or contractual issues;
- Training needs; and
- Recommended changes to policies, procedures, systems, or controls.

The purpose of the review is to strengthen future prevention, response, and recovery.

15. BOARD OVERSIGHT

Administration shall inform the Board of significant cybersecurity incidents and material recovery issues at an appropriate level of detail, consistent with applicable confidentiality requirements, legal advice, public-records exemptions, and the need to protect the security of Odyssey systems.

Board briefings shall be conducted in a public or exempt setting, as required or permitted by applicable law, and any exempt portion of a meeting shall be documented and maintained as required by law.

The Board is not required to approve individual technical response or restoration actions necessary to contain an active incident.

16. ADMINISTRATIVE AUTHORITY

Administration is authorized to take immediate and reasonable actions necessary to protect Odyssey, its students, employees, information, and technology systems during a cybersecurity emergency. Administration is further authorized to establish and revise administrative procedures, emergency response measures, and recovery protocols necessary to implement this policy.

BOARD SECRETARY CERTIFICATE

This Policy was adopted by a majority vote of the Governing Board of Odyssey Charter School, Inc. at a duly noticed public meeting held on September 22, 2026, and is effective upon adoption.

DocuSigned by:
HAIG JOHN
142443FE51CF42A...

Dr. Haig John, Secretary