POLICY & PROCEDURE

TITLE: Data Privacy and Security Policy

APPROVAL DATE OF POLICY REVIEW COMMITTEE: 04/16/2021	**EFFECTIVE/IMPLEMENTATION DATE: 04/16/2021**
APPROVAL DATE OF POLICY REVIEW COMMITTEE CHAIR: 04/16/2021	**POLICY REVIEW COMMITTEE CHAIR SIGNATURE:** Eileen S. Berg

BACKGROUND, PURPOSE & RATIONALE:

The Birch Family Services Data Privacy and Security Policy forms the foundation of the corporate information security program. The policy provides an overview of the principles, processes and solutions that facilitate secure business operations. It also enables the IT organization and senior management the ability to manage the security of information assets and maintain accountability for them.

The Birch Family Services Data Privacy and Security Policy applies to all employees, interns, contractors, vendors and anyone using Birch Family Services technology assets. This policy is used to manage the confidentiality, integrity and availability associated with information assets. Information assets are defined as any information system (hardware or software), data, networks and components owned or leased by Birch Family Services or its designated representatives.

POLICY STATEMENT:

This policy identifies the categories of attack surfaces (platforms and systems that could be vulnerable to cyber-attack), attack vectors (paths by which cyberthreats are enacted) and the processes or technology used to thwart these attacks and protect Birch information assets.

The list of these areas include:

- Network Monitoring and Alerting
- Access Control/Identity Management
- Web Content Filtering
- Patch Management
- Secure VPN Access
- Anti-Spam
- Phishing
- Intrusion Prevention/Detection
- Anti-Virus/Anti Malware
- Data Encryption
- Mobile Device Management
- Security Awareness Training/Testing
- Physical Security (Security Systems/CCTV/Secure Badges/Visitor Access Controls)
- Print/Fax Security
- System Disposal
- Data Backups/Recovery
- Email Security/Encryption
- Secure Wi-Fi
- 3rd Party Security Audit Reports

- Business Associates Agreement
- Network Penetration and Vulnerability Testing
- Multi Factor Authentication

PROCEDURES:

Network Monitoring and Alerting

The IT team actively monitors connectivity and on-premise system availability at all Birch locations using a 3rd party network monitoring and alerting tool. The systems monitored include internet and networking equipment, including but not limited to firewalls, switches and wireless access points. If any of these systems is off-line for more than 5 minutes the IT team is notified via email. Other cloud hosted applications support their own service alerts to identified Birch system administrators and stake holders via email.

Access Control/Identity Management

Various security processes and technologies are utilized to manage on premise and 3rd party cloud (or Software as a Services – SaaS) applications. Non-IT managed systems are administered by a departmental representative. These individuals manage account creation and removal, and access permissions. For IT managed systems, industry standard password complexity rules and access reset policies are enabled as follows:
Standard identity and password complexity requirements include:

- Password History Retention – 8 passwords remembered.
- Required Password Change – every 90 days.
- Minimum Password Length – 9 characters
- Password Complexity Required – at least 3 of the following: Uppercase letter, Lowercase letter, number, special character
- Account lockout duration – permanent until unlocked by either self-service password reset or the IT team if necessary.
- Account lockout threshold – 5 invalid logon attempts

Web Content Filtering

Web content filtering is the practice of blocking access to internet content that may be deemed offensive, inappropriate, or dangerous to employees or the individuals/students we support. Web filtering of unacceptable content is enforced on all internet traffic at all Birch sites through firewall security configurations.

Patch Management

Patch management is the process of periodically applying updates to software and systems. These patch updates are often necessary to eliminate vulnerabilities, resolve application bugs or apply new software features. The Birch IT team automatically deploys patches to all agency managed workstations and servers on a weekly basis using a patch deployment tool.

Secure VPN Access

VPN stands for Virtual Private Network. A VPN secures the connection from a remote PC to the Birch network over the public internet by creating a secure “tunnel” and encrypting the data, shielding online activity from cybercriminals. Birch deploys VPN access to Birch staff requiring secure access to on premise network resources when not at a Birch location. VPN access requires an active Birch network account.

AntiSpam

Spam is the electronic equivalent of junk mail. The term refers to unsolicited, bulk, and often unwanted, email. Birch leverages Microsoft Office365 anti-spam capabilities to minimize spam going to employee email boxes. Birch IT can also manually block any known fraudulent emails or domains as required.

Phishing

Phishing attacks use email with malicious content (links or attachments) to trick employees into divulging credentials to secure information or infecting a Birch computer with malware and viruses. Birch uses various techniques to block phishing attempts. These include firewall rules, email rules, Office365 advanced threat protection features and local anti-virus/anti-malware software on all workstations and servers.

Anti-Virus/Anti Malware

To minimize virus and malware on Birch PCs, Anti-virus/Anti-malware scanning applications are used on all agency issued computer systems and servers. The application is installed on all new equipment and virus definitions are delivered automatically. IT receives regular reports of any virus/malware detected. If necessary, the IT team will follow up with the employee to remediate any potential issues.

Data Encryption

The IT Team encrypts all the hard drives of agency deployed laptops. In the event a laptop is lost or stolen, any data stored on the hard drive becomes inaccessible and can only be recovered with an encryption key that is maintained by IT.

Data stored in the Office365 cloud service is encrypted. Data that moves through the Office365 email system is also encrypted. Enhanced encryption capabilities are available with the Office365 email system for emails that might contain various regulated data types including PHI, HIPAA, FERPA, etc., by adding the word “Secure” or “Encrypt” in the Subject Line of the email.

Mobile Device Management

The IT Team uses mobile device management software (see the Mobile Device Management Policy) to secure all agency deployed smartphones and tablets. Mobile Device Management allows IT to deploy agency approved applications, apply centrally managed security settings and restrict unauthorized applications. IT can also locate lost devices, provide remote support and remotely wipe lost or stolen devices.

Security Awareness Training/Testing

Given the cyberthreats that exist, e.g. Phishing, Social Engineering, Malware, etc., Birch staff are required to participate in semi-annual Security Awareness Training or more frequently as warranted. This training includes a short quiz to verify understanding of the concepts and tactics one can use to recognize these types of threats. Birch also delivers monthly test phishing emails to validate that staff can identify phishing emails. If an employee clicks on an attachment or link in the test email, they are required to take a short remedial refresher training.

Physical Security

Birch Schools and Administrative Office utilize various methods of physically securing the sites. These include a combination of secure swipe key cards, CCTV with remote door lock release, and Intercom systems.

Print/Fax Security

Birch leverages a managed print software application to provide secure print capabilities. All printed documents including PHI or PII require a secure Birch issued swipe card to release the print job. Secure fax services are provisioned using a cloud-based fax service. Documents requiring faxing are scanned to an employee's email and can then be emailed to the fax service (and fax phone number). Incoming faxes go to the email address associated with the Birch fax number and are monitored by key departmental staff.

System Disposal

Given the possibility of computers containing Personal Health Information (PHI), any computers that are damaged, retired or decommissioned, must be disposed of in a secure manner in coordination with the Birch IT Department. Birch employees are not to dispose of, donate or destroy Birch computers. Birch partners with a 3rd party vendor who provides certification of proper green technology disposal and effective hard-drive destruction including a certificate validation of the hard drive destruction, to eliminate the risk of data breach.

Data Backups/Recovery

Birch employs various technologies and services to facilitate data backups and restores for on premise servers and cloud-based data storage. IT staff manage data backups and restores including semi-annual testing based on processes documented in the Birch Data Backup and Restore Policy.

Secure Wi-Fi

All Birch sites have secure Wi-Fi internet access. Birch provides two secure Wi-Fi network names (SSID), one for employees and a guest account for non-staff. Complex passwords are required for access to both networks. The guest Wi-Fi traffic is throttled (or limited) to prevent excessive bandwidth use for non-essential purposes and is separated from the business network to minimize cyberthreats.

3rd Party Security Audits

Birch employs several cloud-based subscription services that host various software services and data. To ensure that system's access and hosted data are secure at their data centers, these providers are required to provide evidence that they are employing acceptable security controls that demonstrate effective security processes that guard against physical or logical infiltration, cyberthreats or other events that might jeopardize Birch information or access to these systems.

A Service Organization Control, or SOC, audit report or similar operating procedure provides guidance to verify that an organization is following specific security best practices. These best practices are related to finances, security (both physical and logical), processing integrity, privacy, and availability. The reports, which are created and validated by third-party auditors, are built to provide independent assurance and to help potential customers/partners understand any potential risks involved in working with the organization. Birch will request a review of a SOC, or similar, security statement that defines these processes prior to vendor selection.

Business Associates Agreement

For service providers that host Personal Health Information (PHI) on behalf of Birch (covered under HIPAA or FERPA regulations), a Business Associates Agreement (BAA) is required. The agreement protects Birch in the event there is a breach of Birch data on the hosting providers system caused by or as a result of actions taken by the business associate.

Network Penetration Testing

Network Penetration scans alert the Birch IT Team to any preexisting flaws in our infrastructure (if they exist) and where they are located. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the networks.

Birch engages with a 3rd party vendor to conduct semi-annual network penetration testing. The test results are used to correct and remediate any gaps in the infrastructure security settings.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is used to ensure that key employees with administrative access to Birch systems and data are required to provide at least two pieces of evidence to prove their identity. The first is a network login challenge and the second must come from a different interaction like an alternate e-mail, text, or phone call. All Birch IT staff are required to use MFA for all Office 365 applications.