1. PURPOSE

Technology is relied upon heavily to collect, store, and manage information. This makes companies more vulnerable to severe security breaches. Information security is defined as the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize a company's reputation. The purpose of the Array Technologies, Inc. Cybersecurity Policy is to protect the company's data and technology infrastructure and maintain the confidentiality, integrity, and availability of IT Resources and data.

2. SCOPE

This policy covers all IT systems and devices that comprise the corporate network or that are otherwise controlled by the company.

3. DEFINITIONS

TERMS	DEFINITIONS
Cybersecurity	Cybersecurity is the protection of computer systems and networks from: information disclosure and theft of or damage to hardware, software, or electronic data.
Anti-Malware	Anti-malware is a type of software program created to protect information technology systems from malicious software, or malware.
Firewall	A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules
Penetration Testing	Penetration testing is the process of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit.

4. REQUIREMENTS

Array IT is required to follow standard cybersecurity procedures described throughout this policy to ensure that they are in compliance with Sarbanes-Oxley.

5. ROLES & RESPONSIBILITIES

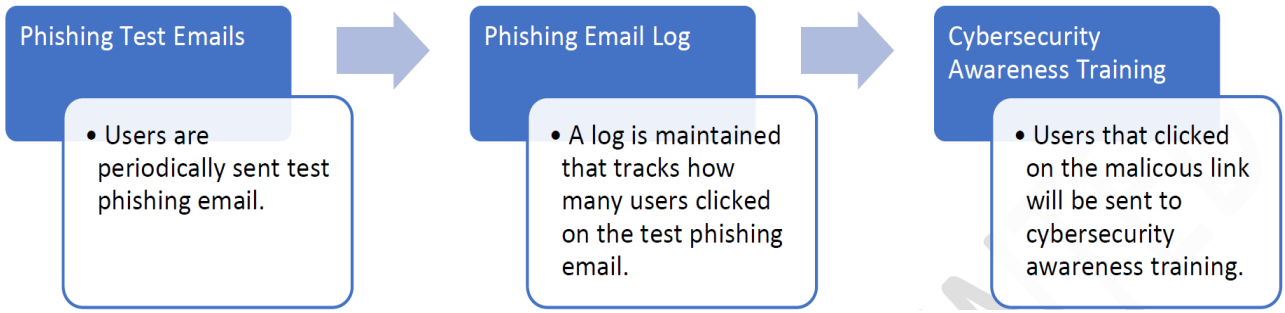
The IT Infrastructure Team is responsible for ensuring that the attributes mentioned in the Cybersecurity policy are enforced. Array IT is responsible for maintaining and updating these policies.

This policy is overseen by the Chief Information Officer at Array. Policy violations should be reported in a timely manner directly to the Chief Information Officer at Jovan.Kangrga@ArrayTechInc.com.

The Chief Information Officer will brief the Audit Committee of the Board of Directors each quarter.

6. WORKFLOW

Cybersecurity Training Process:



7. PROCEDURES

7.1 CYBERSECURITY DESCRIPTION

Cybersecurity is the protection of computer systems and networks from: information disclosure and theft of or damage to hardware, software, or electronic data. The below provides the Company's policies with respect to Cybersecurity.

7.2 ANTI-MALWARE SOFTWARE AND FIREWALL PROTECTION

This section covers the policies pertaining to anti-malware software and firewall protection. For the purposes of this policy, the term anti-malware software includes programs referred to as either: anti-virus; anti-spyware; or anti-malware.

Anti-Malware Software:

- The Company shall ensure that anti-malware software is installed. This applies to all entry/exit points to the network.
- The anti-malware software solution will: inspect network traffic for suspicious domains and IP Addresses; monitor the company's environment; identify and log malicious executable files; and identify critical security incidents.
- To ensure that workforce members cannot interfere with the software's functioning, the Company shall select anti-malware software that can be centrally managed and that cannot be disabled by end-users. The software chosen shall be kept up to date, as new versions are made available.
- At the workstation and server levels, anti-malware protection updates shall be applied through policy settings that are managed by the Doman Administrators.
- The anti-malware software shall be configured to run full system scans continuously or periodically on all workforce member devices. At a minimum, scans for malicious software must be performed on system boots and upon system changes. If malware or malicious code is detected during a scan, it must be immediately quarantined or deleted, and an alert must be sent to the IT Department.
- The Doman Administrators shall review notifications of malware on company information systems and perform appropriate follow-up. Lessons learned from monitoring shall be included in security and awareness training.

- The Company shall ensure that logs from anti-malware scans are maintained for at least one year.

Firewalls:

- Network traffic will be controlled through firewall and other network-related restrictions for each network access point or external telecommunication.
- Routing controls shall be implemented through security gateways (e.g., firewalls) used between internal and external networks such as the Internet and 3rd party networks.
- The ability of users to connect to the internal network will be restricted using a deny-by-default and allow-by-exception policy, based on the requirements of business applications.
- Transmitted information that contains PII (personally identifiable information), banking and/or other sensitive company information will be secured and at a minimum, encrypted over open, public networks by means of end-to-end encryption or by using an SSL secured cloud file transfer site.
- The organization will ensure information systems are protecting the confidentiality and integrity of transmitted information, including during preparation for transmission and during reception.
- The firewall will analyze suspicious code to identify and block newly developed malware from entering the network. These systems will be configured to block potentially malicious files from entering the network and hold the files at the gateway until a verdict is determined regarding the safety of the files. Threat alerts and notifications will be sent to IT Department and all suspicious activity will be actively monitored and dispositioned by the IT Department.

7.3 CYBERSECURITY TRAINING

To ensure that all employees are managing confidential information appropriately, and to mitigate the risk of cybersecurity attacks, we have implemented cybersecurity training for all employees.

Array will follow the below policies:

- All users are required to complete Cybersecurity Awareness training at least annually.
- All users are required to complete phishing training at least annually.
- All users will be periodically notified of new social engineering and/or phishing strategies, as well as new tactics being employed by nefarious groups.
- Users will be periodically sent phishing and scam test emails to provide hands on training and practice. The system will log the number of users that click on links or open attachments from these emails.
- The number of users that click on the links or open the attachments will be updated onto a log for tracking purposes.
- Users will be sent to training if they click on a malicious link. The test emails will be completed as a form of cybersecurity training.

- Users that unknowingly click on phishing links will be provided training on how to be more careful and to be aware of links or attachments that they click on.

7.4 PENETRATION TESTING

Penetration testing is the process of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. The test involves: identifying possible entry points; attempting to break in; and reporting the findings. Penetration testing will be performed annually by the Company.

In addition to penetration testing, Array conducts external assessments and is committed to meeting top information security standards.

7.5 VULNERABILITY SCANNING

Vulnerability scanning will be conducted at least quarterly on all Array subnets and IPs in order to identify all known and unknown devices connected to the Array network and provide vulnerability information per asset. Vulnerability scans are an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. See Vulnerability Management Policy for more detailed information.

7.5.1 INTERNAL VULNERABILITY SCANNING

Vulnerability Scanners will run periodic scans to identify all assets connected to the Array Network and any vulnerabilities identified for each asset.

7.5.2 EXTERNAL VULNERABILITY SCANNING

Vulnerability Scans will be run periodically on all Publicly accessible IP addresses to identify any vulnerable configurations exposed to the internet.

7.6 VIOLATION

Any unauthorized, prohibited, unethical or inappropriate use of Company information assets is a violation of this policy. Violations of this policy may lead to disciplinary action up to and including termination of employment or services.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Additionally, Array is committed to disclosing its practices with external stakeholders. Specifically, we commit to:

- disclosing past material security breaches, along with subsequent policies that were implemented to prevent future violations; and
- implementing whistleblower protections through Array's anonymous whistleblower system to ensure that those who report an internal breach are legally protected.

In addition to the procedures set forth in this Article 7, Array will participate in an information security risk insurance policy to provide Array and its customers with protection in the event of a cybersecurity breach.

8. REVISION HISTORY

RELEASE DATE	REVISION	DESCRIPTION	NAME
6/2/2021	0	Initial Giganet Upload	L. Byrd

06/07/2022	1	Update 7.3 Cybersec training, Added 7.5 Vulnerability scanning	Lorenzo Lopez
12/13/2022	2	Update 5 Responsibilities, 7.4 Cybersec training, 7.4 Penetration testing, and 7.6 Violation	Chris Fox