ARES SECURITY

Protecting the World's Most Critical Assets

Cyber Policy Training

Why are we doing this

- Protection of corporate resources, and government, customer highly sensitive entrusted data.
- Safety act certification.
- Recent issues
  - Compromise of network passwords to Non ARES personnel
  - Ransomware attack on AWS
  - Lost laptops
  - Unencrypted laptop drives
- Continuing Process Improvement
  - What we cover today is the beginning, more to come
  - Tradeoff between burdensome vs necessary
  - Expect some minor policy changes such as O365 policies in Jan

Password Procedures

Responsibilities

- Managers: Managers need to notify IT of any employee status changes, new hires, resignations, terminations or other changes that impact the authorization level of the user on the network.

- IT: responsible for setting up new user accounts including assigning login ID and initial password; managing user id and password policy, removing users from system when the user leaves ARFS Security or commits serious security breach.

- Employees/ Users : Each user is responsible and accountable for their password. Do not share your password. If it becomes necessary to do so, then the users must change their password immediately when shared access is no longer required.

No Generic Passwords

Generic passwords are prohibited.

Examples:

Password!

P@ssw0rd

One2Three4Five#

QWERTY&

LetMeIn!

Trustno1!

Password Aging and Management

- **Passwords will expire every 180 days / users will be notified 14 days prior to the expiration**
- **A minimum of one day must elapse before user may optionally change password**
- **Former passwords may not be chosen upon expiration**
- **10 incorrect login attempts may be attempted before lock out occurs**

Password Protection

Each user is responsible and accountable for their password. Do not share your password. If it becomes necessary to do so, then the users must change their password immediately when shared access is no longer required.

Users must memorize their passwords. Do not place passwords on desks, walls, sides of monitors, or store them in a function or login script, batch file or other communications software.

Examples “WeBedetermined^” “Tomatto(Anvil)” “DOGGed5Astronomer” “Granite&Umbrella2policy”

**Remember that it is easier to remember a password phrase then a password.*

ARES SECURITY

Email and Data Security

All ARES Security employees and subcontractors using an ARES Security information system asset are required to protect the data in accordance with the Cyber Security Manual and this procedure (including referenced procedures).

ARES SECURITY

Email and Data Security

All computer, email and remote access passwords are to be kept confidential

Employees shall not share login and password information with other employees or external parties at any time. Be alert for social engineering attacks.

Extreme care should be exercised when accessing specific types of data or websites with limited protection (HTTP as opposed to HTTPS) or sites that originate from countries outside the US.

All confidential or classified data being transmitted by Email to either non-ARES Security personnel or ARES personnel must be protected in one of the following methods:

- Email encryption (highly recommended)
- Zipped data with encryption and password protection
- Any approved method provided by the client

ARES SECURITY

Email Protection

- **Email usage should be carefully reviewed prior to communication or sending.**

- **Consideration of the content of the email prior to using "reply all" or "forward" is essential. Features are utilized only when all recipients are authorized and need to know.**
  - I did get an email a while ago where an employee, probably on this call, hit reply all when he meant to be private and typed “What is that idiot doing now” It did tell me what he thought of my email, but he probably didn’t mean for me to see it.

- **Emails are considered objective evidence and are admissible in legal actions. Information that cannot be shared publically should not be placed in an email.**

- **Confidential attachments should ALWAYS be password protected and the password sent in a separate email. Also acceptable: Call the receiver of the email and communicate the password to them.**

ARES SECURITY

Suspicious Emails

If an email is received from a party that is unknown OR the email topic / return address does not appear familiar:

1) The email and/or attachment should not be opened.

2) Contact the ARES Security help desk, asc-it@aressecuritycorp.com and allow the ARES Security IT help desk to determine if the email is legitimate.

3) Help Desk will notify the employee of legitimacy of the email and the employee will proceed as directed.

ARES SECURITY

Computer Security

Computers provided by ARES Security or ARES Security customers are to be used for work related purposes

When working in a public area, do not allow access to computer screen. Use of smaller font size and angling away from public viewing are examples of protecting the legibility of the information displayed.

Uploading documents to a server or secured shared sites is recommended to prevent loss of data. Use of storage media until documents can be uploaded should be considered standard practice to prevent data storage on a lap top. Encrypted storage media is recommended.

Employees must lock their computer screen before walking away from their work area.

Never leave a laptop in a hotel room or car unattended. A hotel safe is an acceptable method of storage considering the safe's combination is only known by the employee. Laptops must be removed from parked vehicles and accompany employees at all times.

ARES SECURITY

Use of Personal Computers

If personal computers store corporate documents containing sensitive or restricted information locally, the hard drive must be encrypted. It is preferred that access to these documents be done using the ARES Security VPN to access an ARES Security Server.

Cyber Security and Incident Response Procedure

This policy applies to all offices and equipment, information technology devices and technology systems owned by ARES Security and accessing operational software as well as all ARES Security personnel, contractors and visitors within ARES Security facilities and/or that have access to ARES Security resources.

ARES SECURITY

Cyber Incident Response

- **ALL suspicious computer events/incidents must be reported to ARES Security IT.**

  (CyberIncidentReport@aressecuritycorp.com)

- **In the event of an incident, all computer activity must be halted immediately (which includes not unplugging it from an outlet or the network)**

- **Provide input regarding the incident when suspicious activity is detected as directed by the Incident Responder.**

ARES SECURITY

VPN Procedures

VPN Responsibilities

Any personal system used to access the ARES Security VPN must have anti-virus program installed on their system. These programs must be updated weekly. ARES Security will not be responsible for any problems that may be caused by the use of the ARES Security VPN on a personal computer.

Employees are responsible for using the internet within the ARES Security guidelines while attached to the ARES Security VPN regardless of whether the computer is personally owned or the property of ARES Security.

While attached to the ARES Security VPN, all Internet traffic is routed through the ARES Security network.

ARES
SECURITY

VPN Access

The ARES Security VPN is currently accessible only to authorized users. Currently there is a unique username and password for the VPN, in the future domain authenticated users (logged on with domain user ID, password) will be able to connect from computers that are set up and approved for access via VPN connections. Access to project folders must be granted by the project manager to employees that have a need to know and have met all required security background checks.

IT will set up user ID with permissions to access approved servers and will send instructions and links to the authorized users to initiate VPN access upon request.

ARES SECURITY

Use of the ARES Security VPN

ARES Security Virtual Private Network (VPN), known as the ARES Security VPN, provides employees with remote and offsite secure access to the ARES Security Network, systems, applications and data. The ARES Security VPN is available for all authorized employees to use. ARES Security may refuse to extend remote access privileges to any employee or terminate privileges at any time.

Hardware, software and network services and support provided by ARES Security for VPN use are only to be used for fulfilling an employee's job responsibility. By using ARES Security hardware, software and network systems employees assume responsibility for the appropriate use of the ARES Security VPN, and agree to comply with this policy.

ARES
SECURITY

Authentication and Access Restrictions Procedure

This policy applies to all offices and equipment, information technology devices and technology systems owned by ARES Security and accessing operational software as well as all ARES Security personnel, contractors and visitors within ARES Security facilities and/or that have access to ARES Security resources.

ARES SECURITY

Authentication and Access Restrictions Procedure

Upon the Hiring of a new employee:

Human resources will inform IT to set up new user accounts on corporate servers and permissions on the office server once HR validates the new hire packages.

Upon the termination of an employee.

The manager must communicate the employee's inactive and termination status to Human Resources as soon as the information is known. Any special instructions such as forwarding the terminated employee's email messages to other personnel should be specified.

Human Resources informs IT and provides the employee name, last day of work, and any special instructions.