Information Security Agreement

PURPOSE
To protect Rinker Design Associates' (RDA) information and resources against deliberate or accidental corruption, disruption, deletion, or disclosure from user access of email resources from outside the company

SCOPE
This policy applies to all users of RDA's resources and employees.

RESPONSIBILITY
It is the responsibility of each user to follow the guidelines outlined below when using RDA resources. Violations of this policy may result in loss of network access, disciplinary action, termination of employment or contract, and/or other serious consequences or penalties.

No Unauthorized Use or Activity: RDA prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of RDA information, including but not limited to, trade secrets, sensitive information, and third party information entrusted to RDA employees in confidence. (See handbook for policy details.)

OWA USAGE GUIDELINES

You must use extra caution to protect sensitive or confidential information when accessing e-mail through Outlook Web Access (OWA).

- You must close the Internet browser window to end your OWA session to prevent unauthorized access to your e-mail.
- Do not utilize ANY password saving programs on any computer equipment not defined as official RDA property.

Saving E-Mail or E-Mail Attachments:

- If you are using a PC that is accessible by non-RDA users.by the public or in a public kiosk, you ***must delete*** all copies of e-mail or e-mail attachments from that PC (ex., delete items from Sent Mail). Also, you ***may not*** save e-mail or e-mail attachments to that PC.
- If you are using a home PC or a client PC, you may save e-mail or e-mail attachments, but you must take the responsibility to ensure that those documents are secure as outlined in the policies above.

MANASSAS OFFICE (HQ): 11100 ENDEAVOR COURT, SUITE 200 • MANASSAS, VA 20109
PHONE: 703.368.7373 • FAX: 703.257.5443 • WWW.RDACIVIL.COM

Ensure that the computer you are using has an updated antivirus software package on it prior to access the email system

Using your smartphone or tablet:

- If you choose to configure your smart device to utilize RDA's email access, you acknowledge that RDA has the ability to remote wipe its contacts, emails, and calendar at any time.
- ALL smart devices that utilize an RDA email account must have an initial password set up on that device's home screen that prevents easy unauthorized access.
- Upon the theft of loss of any smart device, you agree to notify RDA's IT staff so they may take the appropriate actions to maintain RDA's network security.

Confidentiality: Users may not divulge their passwords to any individuals unless directed by an approved RDA Manager or by the IT staff

Network Connection: Users must not leave a local or remote connection to the RDA network unattended. The use of screen password protection is strongly encouraged.

Usage: Users acknowledge that they may incur charges when using the email access on their smart devices and that they are solely responsible for the charges (airtime).

Global Protect Usage Guidelines

You must use extra caution while using the Palo Alto Global connect Client (VPN).

- It is the responsibility of the employee with VPN privilege to ensure that unauthorized users are not allowed access to the RDA Network.
- VPN access is controlled using ID and password authentication.
- All traffic destined for the RDA networks is logged and associated with the user.
- Users of this service are responsible for the procurement and cost associated with acquiring basic internet unless provided with a hotspot.

VMware Horizon View

You must use extra caution while using VMware Horizon View

- It is the responsibility of the employee with VMware Horizon View access to ensure that unauthorized users are not allowed access to the RDA Network.
- VMware Horizon View access is controlled using ID and password authentication.
- Users of this service are responsible for the procurement and cost associated with acquiring basic internet unless provided with a hotspot.

All technology provided by RDA, including computer systems, communication networks, company-related work records and other information stored electronically, is the property of RDA and not the employee. In general, use of the company's technology systems and electronic communications should be job-related and not for personal convenience. RDA reserves the right to examine, monitor and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite.

Internal and external e-mail, voice mail, text messages and other electronic communications are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the company.

I acknowledged that I have received, read and comprehend the aforementioned agreement and hereby agree to abide by the guidelines established by the agreement prior to any implementation or usage of RDA's email access and technology.

_____ _____

Signature Date

_____

Print Name Employee #