Richman investments internal use only data classification standard

Technology

Richman Investments " Internal Use Only" Data Classification Standard The " Internal Use Only" data classification standard at Richman Investments will include the most basic IT infrastructure domains to include the User Domain, Workstation Domain, and the LAN Domain. This will encompass all users and their workstations, as well their access to the internet and company server databases and any information in between. The User Domain will enforce an acceptable use policy (AUP) to define what each user can and cannot do with any company data shall he or she have access to it.

As well as with company users, any outside contractor or third-party representatives shall also need to agree and comply with the AUP. All users must be properly identified and sign this AUP prior to gaining any access whatsoever to the company network. No exceptions. Any violation will be taken up with company executives and/or the authorities to assess further punitive action. The Workstation Domain includes all workstations approved on the company network. No personal devices or removable media may be used on this network. All devices and removable media will be issued by the company for official use only.

To access any workstation, a user will need to be first verified, then setup with an account to be logged in with a username and pass code adhering to the IT departments set standards. All systems will undergo regular updates and be provided with anti-virus and anti-malware software for system monitoring. Access Control Lists (ACLs) will be drawn up to appropriately define what access each individual will have. Any violations will cause an immediate suspension of privileges and again the person(s) in violation will be subject to company executives decisions and/or the authorities for punitive action.

The LAN Domain will include all data closets, physical elements of the LAN, as well as logical elements to be designated by authorized personnel. Authorized personnel will be properly screened and authorized by the IT department head and given a special access card with separate pin code as well their normal username and pass code. Each closet will require this special access card and code to gain admittance. Each server will also require this card and code along with separate username and login credentials.

Any hardware, software and equipment is to be installed by these persons only on any machine. Along with that, they will assure proper print, e-mail, and file server setups. They will also be responsible for designating access to users according to ACLs. This includes setup and securing any company Wireless Access Points (WAPs) for use with company devices only. Any violations will be cause for immediate removal of special access rights and suspension of privileges. Again they will be dealt with by company executives and/or the authorities for further punitive action.