HUNT Electric Corporation

ECSI System Integrators

POLICY TITLE: ACCEPTABLE USE

ORIGINAL EFFECTIVE DATE: 12/2004

REVISION DATE: 11/2015

PURPOSE

The computer, network, software, data, contracted services and other information systems, services and equipment (Information Resources) operated by the Company and associated companies are all critical to the success of the Company and must be used appropriately. This policy is designed to protect the Company and associated companies, our employees, customers and other partners from harm caused by the deliberate and inadvertent misuse of our IT systems and our data. Inappropriate use exposes all Users and Information Resources to risks including virus attacks, compromise of network systems and services, financial loss, lost productivity and legal issues.

POLICY

I. Scope of Policy
   A. This is a Company-wide acceptable use policy that applies to all Users and Information Resources.
   B. This policy does not cover use of our products or services by customers.
   C. This policy and its scope are subject to change as technology, business requirements and the legal and regulatory environment develops.

II. Definitions
   A. “Users” are everyone who has access to any of the Company’s Information Resources. This includes permanent regular employees, temporary, variable hour, interns, contractors, agencies, consultants, suppliers, customers and business partners.
   B. “Information Resources” means all information, electronic, computing and communications equipment, facilities, services and software regardless of ownership that operate, connect to or access corporate networks, devices, services and applications that are owned, leased, operated, administered or contracted by or on behalf of the Company. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, software licenses, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, wired and wireless networks, externally provided information services, cloud services and all other similar items commonly understood to be covered by this term.
   C. “Social Media” is defined to include any Internet site or service in which visitors are able to publish content to a larger group. Content shared may include (but is not limited to) personal information, opinions, research, commentary, video, pictures, or business information. Examples of such destinations include large branded entities such as Facebook, Twitter, YouTube and LinkedIn. Blogs, special interest forums, and user communities are also considered social media.

III. Guidelines

A. The Company's Information Resources, including Internet and e-mail, may not be used for transmitting, retrieving or storing of any communications of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual, including remarks of the protected classes within the Title VII of the Civil Rights Act of 1964, shall be transmitted. Harassment of any kind is prohibited.
B. Disparaging, abusive, profane, or offensive language; materials that might adversely or negatively reflect upon the Company or be contrary to the Company's best interests; and any illegal activities, including piracy, cracking, extortion, blackmail, copyright, infringement, and unauthorized access to any computers or resources on the Internet, are forbidden.
C. Copyrighted materials belonging to entities other than the Company may not be transmitted by employees using the Company's Information Resources. All employees obtaining access to other companies' or individual's materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy to reference only. If you find something on the Internet that may be of interest to others, do not copy it to a network drive. Instead, provide the URL (uniform resource locator or "address") and have that person review it on their own.
D. Do not use Information Resources in a way that disrupts their use by others when not work related. This includes excessive Internet usage, sending or receiving many large files and "spamming" (sending bulk unsolicited commercial e-mail messages).
E. Each User is responsible for the content of all test, audio, images and other electronic files that they access, place or send using the Company's Information Resources. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. Also, be aware that the Company's name is attached to all messages to so use discretion in formulating messages.
F. Internal and external e-mail messages are business records that may subject to discovery in the event of litigation. Be aware of this when sending e-mail within and outside the Company.
G. You may use only the computers, computer accounts and computer files for which you have authorization.
H. The Company is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
I. Software or licensed data are subject to the restrictions enforced by the owning entity. Users may not install software or use data that has not been properly licensed for use by the Company or in a manor contrary to the license agreement.
J. You are individually responsible for appropriate use of all resources assigned to you, including the computers, the network address or port, software and hardware. Therefore, you are accountable for all use of such resources. As an authorized User of resources, you may not enable unauthorized users to access the network by using a Company computer or a personal computer that is connected to the Company network.
K. You must not attempt to access restricted portions of the network, an operating system, security software or other Information Resources without appropriate authorization by the system owner or administrator.
L. You may access, use or share the Company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

M. You must not use Company Information Resources in conjunction with the execution of programs, software, processes or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.
N. Company proprietary information stored on electronic and computing devices whether owned or leased by the Company, the employee or a third party, remains the sole property of the Company. You must ensure through legal or technical means that proprietary information is protected. Authorized Company employees may access all such files at any time without knowledge of the Information Resources User.
O. You have a responsibility to respond to promptly report the theft, loss or unauthorized disclosure of the Company proprietary information.
P. The Company reserves the right to monitor and/or log all employee use of Information Resources with or without prior notice. Further, the Company reserves the right to audit Information Resources on a periodic basis to ensure compliance with this policy.
Q. Systems administrators and authorized users must not divulge remote connection VPN, phone numbers or other access points to Company Information Resources to anyone without proper authorization.
R. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), or similar information or devices used for identification and authorized purposes.
S. Users must not make unauthorized copies of copyrighted or Company-owned software.
T. Users may not engage in personal commercial activities using Company Information Resources, including offering services or merchandise for sale.

IV. Incidental Personal Use
A. The Company permits incidental personal use of Information Resources. This means occasional personal use of electronic mail, Internet access, fax machines, printers, and copiers by employees and other specifically authorized Users.
B. Incidental use must not interfere with the normal performance of an employee's work duties.
C. Incidental use must also not results in the direct costs, cause legal action against, or cause embarrassment to the Company and is subject to all of the same appropriate use restrictions as use of behalf of the Company.

V. Social Media/Social Networking
A. The Company recognizes that there are legitimate business and personal reasons for using social media. To enable employees to take advantage of the business value of these sites and to promote an open, trusting, collaborative workplace, the Company policy allows Users to use social media within the guidelines specified above.
B. Corporate Social Media Content
    1. Posting of content to corporate sponsored social media (e.g. the corporate Facebook page) is permitted only by the specifically authorized to publicly represent the Company in these forums.
C. Inappropriate Content Policy
    1. While social media contains legitimate business and personal content, they may also include content that is inappropriate for the workplace including, for example, nudity,

violence, abused drugs, sex and gambling. Therefore, the same inappropriate content rules that apply to general Internet use, also apply to content found within social media.

2. Inappropriate content should not be accessed or created by employees while at work or while using Company resources. In addition to these guidelines, employees should use common sense and consideration for others in deciding which content is appropriate for the workplace.
3. Conduct that is discriminatory, defamatory, libelous or malicious is forbidden. Policies, including but not limited to the Equal Employment Opportunity section of the handbook, Prohibited Harassment Policy and Progressive Discipline Policy apply equally to social networking even if done on nonworking time.
4. The Company may monitor social networking forums and employ technical controls for the purpose of protecting it interests and maintaining compliance with these policies. If employees has any questions regarding this, they should contact Human Resources.

D. Content Publishing and Confidentiality
    1. The following are policy guidelines regarding what you should and should not do when publishing content in Social Media. These guidelines apply to all social media communications whether personal or company-sponsored. Employees are responsible for content they publish in social media and can be held personally liable for content published. Employees also can be subject to disciplinary action by the Company for publishing inappropriate or confidential content. These guidelines only cover a sample of some possible content publishing scenarios and are not a substitute for good judgment.
        i. If you identify yourself as an employee of the Company, the communication must include a disclaimer that the views expressed are yours and do not reflect the views of the Company.
        ii. You may not use and/or disclose confidential or proprietary business information of the Company or its customers, competitors, partners, vendors, and suppliers. Employees are reminded that there are civil and criminal penalties for posting copyrighted material without authorization. When in doubt, always ask permission from the Company's legal department.
        iii. All privacy and confidentiality guidelines in the employee handbook, as well as laws such as copyright, fair use and financial disclosure laws apply to social media.
        iv. Do not comment on confidential financial information such as future business performance or business plans.
        v. Do not cite or reference customers, partners or suppliers without their prior written approval.
        vi. Do not conduct confidential business with a customer or partner business through your personal or other social media.
        vii. Do not register accounts using the Company's brand name or any other unregistered or registered trademarks.

VI. Data Security

A. Users who are supplied with Information Resources by the Company are responsible for the safety and care of that equipment, software, services and data stored or accessed using those

resources, and on other systems that they can use to access the Company's Information Resources remotely.

B. Since information on portable devices such as laptops, tablets and smartphones is especially vulnerable, special care should be exercised with these devices. Sensitive information should be stored in encrypted folders. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems and devices entrusted to their care if they have not taken reasonable precautions to secure it.
C. All workstations (desktops and laptops), tablets and cell phones should be secured with a lock-on-idle policy active after a period of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.
D. Users must not send, upload, remove on a portable media or otherwise transfer to a non-Company system, any information that is designated as confidential or that they should reasonable regard as being confidential to the Company, except where explicitly authorized to do so in the performance of their regular duties.
E. Users are expected to exercise reasonable personal judgement when deciding which information is confidential. Users must take all necessary steps to prevent unauthorized access to confidential information.
F. Users may not store or electronically transmit credit card data unless previously authorized and within the current legal limits of data security. Personal information such as SSN's and medical records are also restricted and should only be stored or transmitted in previously authorized manners.
G. Passwords
    1. Secure passwords are an important contributor to data security. Users are personally responsible for ensuring that their passwords are secure and comply with the Company's password policy.
    2. Passwords associated with an individual User's access to Information Resources may not be shared without authorization from IT. Users may not use another individual's account or attempt to capture or guess other Users' passwords.
    3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. Users must lock the screen or log off when the device is unattended.
H. Malware
    1. New sites, shareware downloads, font sites and social media sites are all commonly used by the online criminal community to deliver malware and carry out schemes designed to damage property or steal confidential information. Users must work to minimize risk related to such threats and adhere to the following guidelines. While these guidelines help to reduce risk, they do not cover all possible threats and are not a substitute for good judgement.
        i. Do not use the same passwords for social media and personal business that you use to access Company Information Resources.
        ii. Do not follow links or downloads software from emails, social media or web pages posted by individuals or organizations that you do not know. Look critically at all links and attachments before opening them.

iii. If any email, social media or web page's content looks suspicious in any way, close your browser or that email and do not return to that page. If in doubt, please contact IT.
iv. When using Company computers off of internal network connections (e.g. home Wi-Fi, Verizon broadband, hotels, etc.) users should be connected to the Company provided VPN at all times.
v. Access social media and web pages through and "HTTPS" address whenever possible. Facebook, Twitter, Google and others support HTTPS encryption as an option. This is extremely important when connecting via public Wi-Fi networks such as those provided by restaurants and hotels.

VII. Privacy

A. No Expectation of Privacy
1. Users should have no expectation of privacy in anything they create, store, post, send or receive using the Company's Information Resources.
2. Users are provided with Computers and access to Information Resources to assist them in the performance of their jobs. All Company Information Resources, including computer systems and company-related work records, belong to the Company and not the User.
3. The Company routinely monitors usage patterns for its e-mail and Internet communications. Since all Company Information Resources, including the computer systems and software, e-mail and Internet connections, are Company-owned, all Company policies are in effect at all times. Employees should use discretion in the sites that are accessed and activities performed using Company Information Resources.

B. Waiver of privacy rights
1. All data stored on the Company's systems is the property of the Company.
2. User expressly waives any right of privacy in anything they create, store, post, send or receive using the company's computer equipment or Internet access. User consents to allow company personnel access to and review of all materials created, stored, sent or received by User through any Company network or Internet connection.

VIII. Cell Phones and Mobile Devices

A. Voice and Data Usage
1. A company issued phone or mobile device is intended for work use. All calls and data usage required to fulfill your specific job duties are permitted. Limited personal usage is also permitted. Video or audio streaming for personal entertainment should never be done with a company owned mobile device, air card or hotspot unless approved in advance. Always connect to WIFI whenever available.

B. Safety concerns with cellphone and mobile device use
2. All employees are expected to follow applicable local, state and federal laws and regulations regarding the use of cellphones and mobile devices at all times. Employees whose job responsibilities include regular or occasional driving and who are issued a cellphone or mobile device for business use are expected to refrain from using their phone or mobile device while driving. Use of a cellphone or mobile device while driving

is not required by the company and safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing a call, accepting a call, texting or typing in an address in a mapping application.

C. Equipment Protection
    1. Employees in possession of company equipment such as cellphones or mobile devices are expected to protect the equipment from loss, damage or theft. Employees are expected to use the company provide protective case for their company issued device at all times.
    2. In the event of a lost or stolen device, employees must contact the Company's IT department as soon as possible.
D. International Travel
    1. Employees should notify the Company's IT department no less than one week before traveling internationally if they are planning to travel with a company owned cell phone or mobile device. If phone or mobile device usage is required while traveling internationally, change to the cellular or data plan will be made to mitigate international charges.
E. Separation
    1. Any phone number on a company owned device is property of the Company. If an employee with a company owned cellular device leaves the company, they can submit a request through their Division Manager to take their number with them. If the request is granted, the employee can move the number to their own device and plan, but the line must stay with the same cellular provider. Hunt Electric will only allow a change of billing responsibility. The employee is responsible for providing the device to transfer service to.

IX. Enforcement of Policy
A. The Company will not tolerate any misuse of its systems and will discipline anyone found to have violated this policy, including not exercising reasonable judgement regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
B. Use of any of the Company's resources for any illegal activity will be grounds for summary dismissal and the Company will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activities.
C. Use of the Company's Information Resources constitutes consent by the User to all of the terms and conditions of this policy.
D. Any exception to the policy must be approved by Company management in advance.
E. Nothing in this policy is intended to prevent employees from engaging in concerted activity protected by law.
F. This Policy should not be construed to ban protected discussion regarding supervisors, management, or in general.

REFERENCES
Progressive Discipline Policy
Prohibited Harassment Policy