Information Technology Unit

POLICY STATEMENT REGARDING APPROPRIATE AND ACCEPTABLE USE OF COMPUTER AND TECHNOLOGY BASED EQUIPMENT AT THE CAREERSOURCE SOUTH FLORIDA ADMINISTRATIVE OFFICES AND CENTERS

Table of Contents

Introduction

The CareerSource South Florida (CSSF) is dedicated to providing the best possible service to its customers and is committed to ensuring that the information system resources are used appropriately and for the purpose they are intended.

This policy governs the use of all computers, computer-based communications networks, and all related equipment administered by CSSF. A user is defined as any person employed and customer served by the CSSF or a CSSF contractor. These include full-time, part-time, temporary, contract employees, and any other individuals working for a partner agency working at a Center or the CSSF Administrative Office.

All equipment is the property of the State of Florida and under the administrative responsibility of CSSF and, as such, all users must abide by this policy. All CSSF facilities and resources are to be used for workforce related business. All equipment users should be aware that any communications or use of the systems and technology resources are not to be considered private or confidential, and can be monitored at any time. For any questions, ask your supervisor or the CSSF IT Unit for clarification or additional information.

Policies Regarding Software

Software, including but not limited to Internet downloads, utilities, add-ins, programs (including shareware, freeware and Internet access software), patches, upgrades, or clip-art, shall not be installed on any desktop, notebook personal computer (PC), or server by anyone other than a representative of the Information Technology (IT) unit of CSSF. There are to be no games on any desktop, PC, or server at any time for any reason. All software purchased for use on the equipment must be approved by the IT Unit of CSSF. Inventory of each PC will be conducted on a regular basis to ensure compliance with this rule.

Licensed or owned software may not be copied to alternate media, distributed by e-mail, transmitted electronically, or used in its original form on other than CSSF PCs without express written permission from the IT Unit of CSSF. In no case is the license agreement or copyright to be violated.

Software licensed to CSSF or its contractors is to be used for its intended purpose according to the license agreement. Users are responsible for using software in a manner consistent with the licensing agreements of the manufacturer.

Policies Regarding Hardware

All PCs, workstations, printers, add-in cards, memory modules, and other associated equipment are the property of the State of Florida and should not be used for purposes other than business. No changes, modifications, additions, or equipment removals may be done by anyone without the involvement or prior consent of the CSSF IT Unit. Network devices such as hubs, switches, routers or any data or voice cables are the responsibility of the CSSF IT Unit and as such, no other staff is allowed to operate the equipment. Contacting IT contractors is the responsibility of the CSSF IT Unit. Under no circumstances should center staff contact IT contractors.

Except notebook PCs used in daily offsite work, no equipment should be removed from its premises or within the premises without the authorization of CSSF IT Staff. In the event equipment is to be off premises for work related purposes, a request must be made by the Center Manager to the CSSF IT Unit with appropriate justification and a copy of the same must be forwarded to the CSSF Facilities Manager for approval.

It is prohibited to install any wireless devices without prior consent and involvement of the IT Staff. It is also prohibited to tamper with any device or device configuration.

All Centers are required to secure the telephone/data wiring room with a lock. The lock must be accessible on-site by the person managing the center. If the room is not locked, contact the CSSF Facilities Manager so that preparations can be made to lock the room.

Beverages and food are prohibited near the equipment.

Best Practices

User access codes and passwords are for the use of the "*specifically assigned user"* and are to be protected from abuse by unauthorized individuals. User names and passwords to the network and to all systems must not be shared with other staff or anyone else other than the intended user.

Users must logoff from their workstations at the end of the each day or when away from their workstations for extended periods of time to minimize security risks.

All diskettes, e-mail attachments and executable e-mail messages should be automatically scanned for viruses using the virus detection software installed on the computer workstations. If you have made any configuration changes to your workstation, even with the approval of the IT Unit, it is your responsibility to ensure virus protection prior to opening/executing diskettes, e-mail attachments or executable e-mail messages.

Like all CSSF information systems resources, Internet access and e-mail are for work-related use. Emails and sites visited can and will be monitored on a periodic basis.

Employees may not use CSSF system resources for soliciting, personal financial gain, partisan political activities or further disseminating "junk" e-mail such as chain letters. Email accounts will be disabled for a period of 30 days for those employees who do not adhere to this policy.

Information contained on the CSSF network and workstations is strictly proprietary to the State of Florida and CSSF. Copying or disseminating any of this information for any purpose other than CSSF/State of Florida business is strictly prohibited. Access to this information must be considered confidential.

You are expected to report policy violations, which you observe to your supervisor or, in the event that the violation involves the supervisor, the CSSF IT Unit or CSSF Management. Likewise, if you are a witness to a violation you are required to cooperate in any investigation of the violation.

Consequences

Any user who knowingly and willingly violates this policy is subject to disciplinary action up to and including termination from employment depending on the severity of the specific offense(s). Furthermore, in the event of an illegal activity, the user will also be reported to the appropriate law enforcement authority. If you have any question regarding this policy or any situation not specifically addressed in this policy, see your supervisor or the IT Unit of the CSSF.

Revisions

This policy is subject to revision. CSSF will adequately post revisions on its website, but it is the user's responsibility to ensure that all of the computing and communication resources conform to current policy.