Version Number 6.0
Owner: I.T. Security Director
Document Number: TJG-POL-004
Effective Date: Jan 1 2015

CONSULTING * STAFFING * TRAINING

People Powered Business Solutions

Contractor Cyber Security Policy

Our Company:

The Judge Group is a privately-owned, leading professional services firm. What does that mean? It means we provide technology, talent and learning solutions to businesses around the globe, and we're great at it. Our expertise is positioned at the crossroads of people and technology - two of the most important aspects of successful business today.

At Judge, Cyber Security and Information Management are part of our core values. Our ISMS are designed and implemented to adhere to ISO27001 (ex. BS7799-2) and ISO27002 standards.

Scope:

This policy establishes the basic principles necessary for the secure use of “Client” information and information systems. This policy applies to all contractors at all locations, directly placed by The Judge Group.

Workforce Management:

1. All “the client of Judge for whom you will be performing services (“Client”)” information assets (e.g. data, databases, reports, emails, instant messages, manuals, systems documentation, procedures and plans) are considered **strictly confidential** unless expressly stated otherwise by “Client” in writing.
2. Contractors are responsible for protecting all “Client” information and the systems which process, store and transmit such information from unauthorized disclosure.
3. The “Client” Project Manager is responsible for determining the access rights to information systems and for granting Judge Contractors appropriate access rights and usage permissions.
4. Judge Contractors must abide by all Institutional policies already in place.
5. Judge Contractors may not use “Client” systems to knowingly compromise other “Client” systems, networks or safeguards.
6. All “Client” information systems (email, internet, telephones etc.) are the property of “Client” and are primarily for the explicit use of “Client” business. Judge Contractors must never use them to knowingly access, store or distribute pornographic or otherwise offensive material.
7. Judge Contractors are expected to make every effort to ensure that all “Client” information is protected from inadvertent disclosure when being sent over the Internet or other open, non-”Client” networks.
8. Encryption or password protection must be used when available to protect “Client” information.
9. Any unauthorized attempt to access information considered outside the Contractors project requirements is prohibited.
10. All Judge Contractors are responsible for safeguarding their passwords, user IDs and badges and protecting them from unauthorized use.
11. All Judge Contractors are prohibited from disclosing or sharing passwords or user IDs with anyone.
12. Any unauthorized attempt to discover the password of another user or to access “Client” information or “Client” systems using another person’s password or user ID is prohibited.

13. Judge Contractors may not use “Client” email or computer systems to send any personal, business or any other type email to personal or non-client business email recipient accounts.
14. All Judge Contractors are prohibited from introducing viruses or malicious code into “Client” systems, software, or devices. This includes peer-to-peer file sharing programs.
15. All Judge Contractors are prohibited from attempting to bypass “Client” virus protection software or other system safeguards (e.g. when downloading or transferring information).
16. When available, Judge Contractors must always use installed virus protection software and other system safeguards.
17. All Judge Contractors must scan all files and software before introducing them to “Client” systems.
18. Judge Contractors must not install or use non-certified software (i.e. software that is not licensed) for any purpose unless specifically granted an exception that is authorized by their Project Manager.
19. To ensure information security and integrity, Judge Contractors must always completely log out from all applications and leave desktop computers in the locked screen state when leaving their work areas for breaks or lunches.
20. All systems and software packages must be fully tested for system compatibility by the “Client” Information Technology Team before deployment.
21. Judge Contractors will comply with all documented processes for information removal/destruction (both electronic and printed formats).
22. Judge Contractors may not remove equipment from “Client” facilities without written authorization from their Project Manager.
23. All information security incidents (e.g. malicious code, worms, viruses, unauthorized or inappropriate email/internet use) must be immediately reported to a Project Manager upon discovery.
24. Loss of desktop, portable, or mobile computing devices by any means (e.g. theft, loss, breakage) must be reported to the Project Manager as soon as discovered to ensure that all network access is disabled.
25. It is Contractor’s responsibility to return all equipment provided in the condition it was given. Other than normal wear and tear, if any damage is done to the equipment while in Contractor’s possession or if Contractor fails to return it, Contractor shall be liable for the cost to repair or replace it.
26. Contractor certifies that he or she understands this policy and agrees to be bound by it. Contractor accepts all liability that arises as a result of his or her breach of this cyber security policy.

Printed Name

____

Signature

____

Date

____