Security Policy Manual

The Judge Group

151 South Warner Rd Wayne, PA

Version 2.2

Quarter 1 2024

By Paul Bettinger

CEO	DocuSigned by: Martin E. Judge III	Feb 2024
CIO	DocuSigned by: David R. Armstrong	Feb 2024
ISO	DocuSigned by: Paul T. Bettinger	Feb 2024

Contents

1. Executive Summary

In the 20th Century Abraham Maslow's Hierarchy of human needs was a theory he developed that stated human motivation is based on people seeking fulfillment and change through personal growth. Many adaptations of this theory now exist including some used in Corporate Leadership training courses. A simple Google search of" leadership training based on Maslow's hierarchy of needs" will return many results. Maslow's hierarchy is organized as a pyramid (*see appendix A*) with basic needs such as air, water, and food forming the base. The second tier of need is **security**. Curiously, this broad need disappears in many corporate leadership training courses or is listed as a poor disengaged employee state if mentioned at all. Security is a critical need that both individuals and organizations must account for to be the best that they can be.

Security is a collective enterprise with all people sharing some responsibility. This is true from individuals to family, community, state, and country, all the way up to the planetary level should the security threat be large enough. This is not an easy concept to grasp given the siloed and divisive environment that exists in society. In the corporate environment, security is also a shared responsibility because if one company experiences a serious security incident this potentially affects its business partners and customers in the supply chain. All participants in the supply chain have a responsibility not to jeopardize the chain. The further up the chain that a company progresses the greater care it must take to ensure that it and its' partners protect the chain. Legally the Chief Executive Officer and Senior Management team is held responsible for ensuring that the company exercises due care with regard to protecting its' clients and customers. With support of senior management, the security team devises and implements a security program to help ensure that under legal scrutiny the company can in good faith be seen to have acted prudently, thereby reducing the risk of severe criminal or financial punishment in the event of a severe security incident.

The Judge Group now has more than fifty years of operational expertise and is committed to ensuring the confidentiality, integrity, and availability of systems and data that support our operations and the needs of our clients. The Judge Group continues to invest the needed resources in tools and infrastructure to guarantee the dependability that our clients look for in a caring and trusted partner. The thoughtful application of the security policies contained within this manual underscore the Information Security team's desire to empower The Judge Group to achieve its' business objectives and allow the organization to persevere in the event of disaster. The Infosec team strives to collaborate with other departments within The Judge Group to promote security awareness and continually improve our security practices.

If you require additional information or would like to request access to audit or other regulatory information, please email infosecteam@judge.com

Kind Regards,

Paul Bettinger, Information Security Officer

The Judge Group 2023

2. Policies

1. Overview

Policies are pre-defined principals and courses of action tailored to meet specific physical, mental, or existential needs. Governments, businesses, groups, and individuals develop policies to increase operational efficiency, assist in decision making, and provide collective understanding to groups so that they can better align to achieve goals as well as comply with legal and ethical responsibilities.

2. Purpose

The purpose for this policy is to establish a common format for Judge Group Information Security Policies to promote an accessible, consistent, and understandable policy framework.

3. Scope

This policy applies to all policies recorded and maintained in the Security Policy Manual.

4. Policy

4.1 Policies published to the Security Policy Manual are meant to promote operational efficiency, reduce risk, help ensure legal compliance, promote ethical standards, enable operational integrity and as such should be supported by Senior Management.

4.2 All employees and affiliates should be familiar with the specific policies that relate to their functions, duties, and relationship to the company.

4.3 Compliance with policies should be compulsory unless a specific exception is granted by a company officer, legal agent, or senior management.

4.4 Policies should be reviewed for accuracy and relevance on an annual basis.

4.5 Unless otherwise stated, the responsible party listed in the history table is the Owner of the policy.

4.6 The standard outline for published policies should consist of the following sections: Overview, Purpose, Scope, Policy, Compliance, Related Standards, Definitions, and Revision

4.7 The Information Security Officer or delegated agent should publish policies to the manual.

4.8 Distributed copies of policies should be considered invalid\obsolete one year from the printed date.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy annually via internal audit.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2022	Steven Clymer	Initial Release
February 2024	Paul Bettinger	Reviewed

2.1.Roles

1. Overview

We are all part of one community or another. Each member of a community fills a role within that community to support the goals that brought the community together. Security is a community affair and everyone in the community has a role to play in keeping the community safe.

2. Purpose

The purpose of this policy is to define the Information Security roles and responsibilities of The Judge Group community to ensure all members understand what their contributions to the confidentiality, integrity, and availability of Judge data and systems entails.

3. Scope

This policy applies to all Judge Group employees and affiliates.

4. Policy

4.1 **Users:** Anyone and everyone who accesses Judge Group facilities, systems, or data. All Users are required to adhere to the policies detailed in this manual. Anyone utilizing Judge Group systems should apply prudence to their actions to safeguard people, data, and systems. No Users should purposefully try to inflict harm.

4.2 **Custodians:** In addition to the responsibilities of Users, Custodians are charged with designing, implementing, maintaining, and managing Judge Group systems and data with focus on the security program while fulfilling their daily functions. Custodians devise procedures to comply with security and facilitate operations.

4.3 **Privacy Officer** is responsible for ensuring The Judge Group remains compliant with information privacy laws and regulations. The Privacy Officer will provide guidance for privacy awareness training for all Judge Group staff.

4.4 **Information Security Officer** is responsible for the development, implementation, and maintenance of The Judge Group information security program.

4.5 **Chief Information Officer** will be kept informed of information security activity, provide prioritization of resources, and supply executive oversite to The Judge Group Information Security program.

4.6 **Chief Executive Officer** bears the primary responsibility for the safety of all Judge Group people, data, systems, and facilities. In the absence of a named CISO the CEO is legally considered to hold this role as well. Without the support and sign off the Chief Executive no security program can be successful.

5. Policy Compliance

5.1 Compliance Measurement

The above listed officers will ensure compliance through various methods.

5.2 Exceptions

5.3 Non-Compliance

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2022	Steven Clymer	Initial Release
February 2024	Paul Bettinger	Reviewed

2.2.Security Policy

1. Overview

Operating in a secure manner is fundamental to the safety and profitability of any commercial enterprise and providing clearly defined expectations of security parameters is essential. Security policies provide the broad instruction set for security and information workers to organize their focused efforts to maintain the confidentiality, integrity, and availability of company data and systems.

2. Purpose

The purpose of the security policy, along with its' related polices, is to define the provisions under which the company operates to achieve its' core mission as well as maintain the confidentiality, integrity, and availability of data and systems. Reduction of risk, enumerating access and roles, defining system and application standards as well as response to threats or disasters needs to be detailed to provide a workable framework of enforceable actions and consequences to ensure continued success.

3. Scope

This policy applies to all Judge Group employees, contactors, third-party affiliates, systems, applications, and facilities both domestic and international.

4. Policy

4.1 All systems owned by the company can be accessed by IT admin staff at any time and no expectation of privacy should be expected.

4.2 An accurate accounting of all assets should be maintained and their role and importance to the operation of the company should be classified and reviewed on a periodic basis.

4.3 Information security efforts should align with company objectives and those objectives should be clearly communicated by the business so that proper resources can be allocated, and informed risk decisions can be made.

4.4 The infosec team is responsible for presenting meaningful risk information to the business so that tolerances, and priorities can be established to make sound risk decisions.

4.5 Access to company physical and logical assets may only be granted to authorized subjects.

4.6 A continual education effort must be undertaken to make all staff, senior leaders, and third-party affiliates aware of security duties and responsibilities.

4.7 Data must be managed to ensure the confidentiality, integrity, and availability of company information.

4.8 Clearly defined procedures need to be maintained for the management of information systems.

4.9 Information Technology staff must perform regular system maintenance to ensure operation of systems and maintain record of maintenance levels.

4.10 Infosec staff must monitor systems in a consistent manner to identify events and report on findings.

4.11 Event findings must be analyzed to understand impacts.

4.12 The team responding to incidents needs to be supported by senior management so that it can react in a timely manner, communicate events clearly and to mitigate events based on their impact.

4.13 A recovery plan must be maintained and tested to ensure systems and operations are restored in an acceptable time frame when an event occurs.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, tool reports, internal and external audits, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the CEO, CIO, or ISO in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2022	Steven Clymer	Initial Release
February 2024	Paul Bettinger	Reviewed

2.3.Risk Management Policy

1. Overview

Every action or inaction carries with it some level of risk. Once a risk is identified it must never be ignored. The appropriate responses to risk are avoidance, acceptance, reduction, and transference. Selecting the best response will help maximize the chance of a positive outcome for all risks encountered.

2. Purpose

The purpose of this policy is to establish a framework under which the Infosec team can perform risk assessments to determine areas of vulnerability and react with appropriate remediation steps to minimize residual risk to an acceptable level. Timely and thorough practices are important to ensure that the Judge Group takes due care to protect Judge Group and customer data.

3. Scope

This policy applies to all Judge Group systems, applications, and facilities both domestic and international. Risk assessments can be conducted on any information system, server, application, network, or procedural process in production or being evaluated by The Judge Group.

4. Policy

4.1 Risk assessment and remediation is a joint responsibility between Infosec and The Judge Group department, entity, custodian, or owner of the target of assessment.

4.2 Employees must cooperate with individuals granted rights to perform risk assessments regardless of whether they are internal or external personnel.

4.3 It is incumbent upon the responsible party to work with the Infosec team to come up with and execute a remediation plan.

4.4 Risk assessments must be carried out periodically to account for changes, new needs, and potential shifts in risk.

4.5 A security assessment should be included in the initial phase of any project to ensure that due care is taken while conducting company operations.

4.6 A systematic approach should be taken when conducting risk assessments that can be repeatedly followed to produce consistent results.

4.7 Findings from completed assessments should be presented to senior management or stakeholders to sign off on whether risk should be avoided, reduced, transferred, or accepted.

4.8 Risk reports should be kept for five years.

4.9 Automated risk tools should be deployed where practical and possible to provide on demand or scheduled risk assessments of critical systems.

4.10 Risk reports should be detailed based on the audience reviewing the findings.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, tool reports, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the CEO, CIO, or ISO in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

Appendix B Risk process.

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.4. Data Management Policy

1. Overview

In the 21st century data is what empowers leaders to make decisive decisions to accomplish core objectives and gain competitive advantage over rivals. Data represents the second most valuable asset of an organization. Understanding what data is available, how it is used, and how to protect it is vital to the success of any group.

2. Purpose

The purpose of this policy is to provide guidance about how Judge Group data should be governed, protected, and classified so that it is not, and does not cause harm to The Judge Group, affiliates, or customers.

3. Scope

This policy applies to all Judge Group structured and unstructured data stored or transmitted by any system owned or leased by The Judge Group and its affiliates. Any customer data that is stored or processed by Judge systems or staff should be afforded the same level of care with regards to protection.

4. Policy

4.1 All data created or collected by The Judge Group and its affiliates is owned by The Judge Group and not any specific person, department, or business unit within the enterprise. This applies to both structured and unstructured data. Customer data that The Judge Group is temporarily custodian of remains the property of the customer or client.

4.2 The Judge Group shall only collect data deemed relevant to the services that the organization provides and shall ensure that collected data complies with applicable laws and regulations with regards to collection, storage, and destruction.

4.3 The three classification levels of data in use at The Judge Group are confidential, restricted, and public.

4.4 All Judge Group data should be assigned a security classification appropriate to its' importance to the company.

4.5 Data that no longer has any value to the company should be destroyed and all data should be periodically assessed for quality to determine the current value of the data.

4.6 Retained data should be encrypted to meet current industry standards to ensure confidentiality at all times. The current minimum-security standard is AES with a 256bit encryption key.

4.7 All data should be reliably backed up on at least a daily basis and routinely restored to ensure a high level of integrity and availability.

4.8 Due care should be taken to reduce the number of duplicate data sets to reduce costs, ease management and increase the overall security of Judge Group data.

4.9 Data should be modeled in a consistent format so that structured data can be more easily shared and reused. This will increase efficiency and foster a better organizational wide understanding of company data and its value.

4.10 All company documents should have some level of version control applied to maintain integrity and to provide historical record of evolving changes.

4.11 Custodians shall develop, maintain, and record levels of access rights and privileges to data sets.

4.12 Custodians are responsible for ensuring that only authorized personnel, in a proper role, will be granted access to data sets.

4.13 Users shall be given the least amount of access to data that their specific function requires to complete successfully.

4.14 Paper records should never be used to store anything other than public data and paper used to record any other data type must be destroyed within thirty days by cross shredding or complete disintegration.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, tool reports, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the CEO, CIO, or ISO in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including legal prosecution.

6. Related Standards, Policies and Processes

7. Definitions and Terms

7.1 Confidential: Data that is considered legally regulated and /or data that could be used to identify a specific individual or data that is considered essential to the vitality of business operations.

7.2 Restricted: Data that custodians have decided should not be made available to staff in general but can be disclosed to groups or individuals when business needs require access be granted.

7.3 Public: Data containing no confidential or strategic value that requires no access restrictions.

7.4 Retained Data: Any data at rest that is stored on Judge Group systems.

8 Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.5.Access Control Policy

1. Overview

Access control has been a security concern since the formation of societies. Proper implementation of access control ensures that people, data, facilities, and systems stay safe and secure. Access controls come in both physical and logical forms. Consideration needs to be given to both forms to be effective.

2. Purpose

The purpose of this policy is to detail the required minimum physical facility standards and data access controls to be instituted by The Judge Group to properly protect employees, facilities, and ensure the confidentiality, integrity and availability of systems and data.

3. Scope

This policy applies to all Judge Group facilities and datacenters both owned and leased as well as all Judge Group systems and personnel worldwide.

4. Policy

4.1 Physical access control

4.1.1 To be consistent with other policies, Judge Group facilities should be divided into three security zones, public, restricted, and confidential.

4.1.2 Reception, restroom, break, and lobby areas should be considered public areas and any conversations about restricted or confidential data should not take place in these areas. Anyone coming into the public space should be identified and their arrival and departure recorded.

4.1.3 Restricted areas consist of all workstations, collaborative, and office spaces within Judge owned or leased facilities. Only Judge employees and trusted third parties should be allowed to move around company spaces unescorted. All guests should be accompanied by Judge staff while in restricted areas. Doors in restricted areas shall be secured at all times.

4.1.4 Confidential areas such as MDFs, IDFs, IT closets, electrical, and mechanical rooms should always be secured, and access restricted to specific individuals whose occupation require access to those facilities. Third party affiliates must be accompanied should they need to work in confidential areas. Confidential areas should be secured so that individual access can be audited.

4.1.5 Should The Judge Group commission a secure hardened facility, Infosec should be involved in the initial planning and site selection. Infosec should work with the facility team to ensure that any selected site follows CPTED and Infosec shall provide a secure facility plan based upon the business requirements of the facility.

4.1.6 All Judge leased or owned facilities shall comply with all local zoning, electrical, mechanical, civil, and fire safety codes. All fire suppression systems must be inspected and maintained per local codes.

4.1.7 All issued physical access devices, access tokens and keys, must be kept secure and promptly reported should they be lost or stolen. Upon termination of relationship any issued device should be deactivated or returned.

4.1.8 In Judge controlled facilities access groups should be created and assigned to control which area of a facility staff may access based upon their role.

4.2 Logical Access Control

4.2.1 Before any authentication credentials can be assigned the subjects' identity must be verified. The level of identity assurance must meet company compliance standards based on the privilege level of access being assigned.

4.2.2 Once identity has been verified, a request for access can be submitted to the IT department provided all required information is available.

4.2.3 The IT department will trigger the IAM to create a user account based upon the role information provided in the access request.

4.2.4 All user accounts should be created using the RBAC templates within the IAM. As new roles are needed, the Infosec and Sysops team can create new templates based upon the identified least privilege access to systems and applications required to complete the new roles' responsibilities.

4.2.5 All new templates created should be reviewed by IT management to ensure least privilege is followed before the new template is committed for use.

4.2.6 Any accounts that need to be created via discretionary access must be approved by the ISO with documentation provided why the standard RBAC templates can't be used.

4.2.7 Any existing accounts that require discretionary access to be granted must get approval by the ISO or another authorized agent.

4.2.8 No shared accounts shall be used to access Judge Group infrastructure or data systems.

4.2.9 All non-permanent staff accounts will be set to expire based upon their expected engagement.

4.2.10 If a person changes role within the company their access rights should be removed and reprovisioned with the rights from the appropriate RBAC template.

4.2.11 All user accounts should be periodically checked to ensure their access rights match any change in responsibility.

4.2.12 User accounts should be deactivated in a timely manner when the account is no longer needed, or the account holder ends their engagement with the company.

4.2.13 Accounts attempting to access systems with five or more failed attempts in five minutes should be locked for at least thirty minutes from attempting access again.

4.2.14 Accounts connected to resources should reset when 15 minutes of inactivity is reached.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the CEO, CIO, or ISO in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.6. Password Policy

1. Overview

Passwords still represent the first and most common method to secure and provide access to systems or services. Poorly designed and managed passwords put everyone at risk.

2. Purpose

The purpose of this policy is to provide clear guidance about how Judge Group passwords should be implemented and managed.

3. Scope

This policy applies to all Judge Group staff, contractors, and affiliates.

4. Policy

4.1 Weak passwords cannot be used for any system or account in the organization. Weak password examples include passwords of less than eight characters, passwords that contain personal information such as birthdays or names, passwords with recognizable patterns such as qwerty or abcd1234.

4.2 Strong passwords represent the minimum requirement to access any system or services in the organization. Examples of strong passwords include passwords of more than 8 characters, passwords that consist of phrases, and passwords that consist of combinations of upper- and lower-case letters, numbers, and symbols.

4.3 **All passwords must meet the following criteria: 8 or more characters, both upper- and lower-case letters, at least one number, and at least one special character**.

4.4 Passwords will expire every 90 days.

4.5 Passwords cannot be reused for at least 6 password cycles.

4.6 **Under no circumstances should your password be given to anyone**.

4.7 You should never use a password from your Judge Group account for any non-Judge Group account.

4.8 Your password should be memorized and never written down.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team verify compliance to this policy through various methods, including but not limited to, tool reports, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.7.Acceptable Use Policy

1. Overview

The intention for publishing an Acceptable Use Policy is to protect employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of The Judge Group. These systems are to be used for business purposes in serving the interests of the company, our clients, and customers. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of The Judge Group's computer systems. These rules are in place to protect the employee and the company. Inappropriate use exposes The Judge Group to risks including malware, compromise of network systems, services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by the Judge Group, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at The Judge Group and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with The Judge Group policies and standards, as well as local laws and regulations. This policy applies to employees, contractors, consultants, temporaries, and other workers at The Judge Group, including all personnel affiliated with third parties.

4. Policy

4.1 General Use and Ownership

4.1.1 Judge Group proprietary information stored on electronic and computing devices whether owned or leased by The Judge Group, its' employees or a third party, remains the sole property of The Judge Group. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Judge Group proprietary information.

4.1.3 You may access, use, or share Judge Group proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Judge supplied computer equipment is meant to be used for the performance of individual job responsibilities and not general personal use. All employees are responsible for exercising good judgement with regards to personal use and no such use should conflict with any Judge policy or regulations. Upon completion of an engagement with The Judge Group, all company owned equipment must be returned in a timely manner and in good condition.

4.1.5 For security and network maintenance purposes, authorized individuals within The Judge Group may monitor equipment, systems, and network traffic at any time without prior notice.

4.1.6 The Judge Group reserves the right to audit networks and systems to ensure compliance with this and other policies.

4.2 Security and Proprietary Information

4.2.1 Only Judge owned and maintained mobile devices may connect to the Judge internal wireless network and any non-Judge device may only use guest wireless access.

4.2.2 System level and user level passwords must meet the following criteria be a minimum of 8 characters long, contain both upper- and lower-case letters as well as a number and a special character.

4.2.3 All computing devices must be secured with a password-protected screen saver with auto activation set at no longer than 15 minutes. Employees must lock their screen or log off when the device is unattended.

4.2.4 Postings by employees from a Judge Group email address to newsgroups, social media or other external sites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of The Judge Group, unless posting in an official course of business duties.

4.2.5 Employees must use extreme caution when opening email attachments as they may contain malware

4.3 Unacceptable Use

4.3.1 The following activities are, in general, prohibited. Employees may be exempted from these restrictions while performing their legitimate job responsibilities. **Under no circumstances is an employee of The Judge Group authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Judge Group owned resources**. The lists below are not complete lists but an attempt to provide a framework for activities considered unacceptable use.

4.3.2 System and Network Activities that are strictly prohibited with no exceptions:

a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by The Judge Group.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which The Judge Group or the end user does not have an active license is strictly prohibited.

c. Accessing data, a server, or an account for any purpose other than conducting Judge Group business, even if you have authorized access, is prohibited.

d. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
e. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
f. Revealing your system or account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
g. Using a Judge Group computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
h. Making fraudulent offers of products, items, or services originating from any Judge account.
i. Signing up for any service or site with a Judge Group user or email account unless that site or service is directly related to legitimate job functions.
j. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
k. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
l. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
m. Connecting any non-Judge owned equipment to the Judge network without prior authorization
n. Introducing honeypots, honeynets, or similar technology on the Judge Group network.
o. Interfering with or denying service to any user. (Example, denial of service attack).
p. Installing any unauthorized software on Judge Group systems.
q. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
r. Providing information about, or lists of, Judge Group employees to parties outside of the Judge Group unless this is for legitimate Judge Group business.
s. Downloading and storing customer or client data onto a Judge workstation or onto personal file space is prohibited.
t. Usage of AI tools, including but not limited to ChatGPT, is prohibited within the company premises. The sole approved AI for company-related tasks is the Company Supported AI (Microsoft CoPilot). Any exceptions to this policy must

undergo thorough review by company leadership and the Information Security (InfoSec) team.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including legal prosecution.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Added line item regarding AI usage "t"

2.8. Clean Desk Policy

1. Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use, or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers, and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

3. Scope

This policy applies to all Judge Group employees and affiliates.

4. Policy

4.1 Sensitive information shall not be left unattended so employees must secure any such information before leaving their desk or leaving open workspaces in Judge facilities.

4.2 Sensitive information includes but is not limited to name, address, social security number, date of birth, driver's license number, passport number, or any image displaying personal information.

4.3 Documents containing sensitive information should be placed in locked bins and then shredded when no longer needed.

4.4 Computers should be locked when leaving the workstation for any reason.

4.5 Sensitive information should only be sent to secure print stations.

4.6 Any restricted or sensitive information must be removed from the desk and locked in a secure location at the end of the day.

4.7 File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.

4.8 Keys used for access to restricted or sensitive information must not be left at an unattended or unlocked desk.

4.9 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down.

4.10 Whiteboards containing restricted and/or sensitive information should be erased after use.

4.11 Lock away portable computing devices such as laptops and tablets.

4.12 Treat USB drives as sensitive and secure them in a locked drawer.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.9. Endpoint Control Policy

1. Overview

After people, endpoints pose the most significant danger to the security of data and systems. The sheer volume and diversity of devices that potentially get connected to company infrastructure mandates that clear control and accountability of those devices is required to protect the infrastructure.

2. Purpose

The purpose of this policy is to establish the minimum requirements for all endpoints that utilize The Judge Group networks to gain access to services supplied by systems to ensure that the integrity and availability of those systems are not compromised.

3. Scope

This policy applies to all Judge Group employees and affiliates across all sites.

4. Policy

4.1 The Judge Group does not have, nor does it support a **BYOD** environment

4.2 Limited guest wireless internet access is provided on a separate SSID from general Judge wireless access.

4.3 Non-computer endpoints such as VOIP telephones, IoT devices, APs etc. should be checked at least twice annually to ensure that operating firmware is the most up to date and secure version available from the device manufacturer.

4.4 Any devices that no longer have supported firmware and are considered end of life by the manufacturer should be replaced as soon as resources are available to do so.

4.5 Only Judge Group owned, sanctioned, or managed equipment is authorized to be connected to Judge Group internal networks.

4.6 Infrastructure and Infosec staff shall work together to actively ensure that rogue endpoints connected to Judge networks are discovered as quickly as possible and actively denied that connection.

4.7 All personal computers and laptops in use must run legally licensed, currently supported versions of a Judge Group standard OS.

4.8 The standard OS for personal computers and laptops at the time of this writing is Microsoft Windows 10.

4.9 A standard baseline image should be maintained for all endpoint devices.

4.10 All endpoint computer devices should be routinely examined and kept up to date on drivers and software patches.

4.11 Machines should be configured with a baseline install of software and settings and this should be cataloged in a controlled repository.

4.12 All user endpoint computers must have an up to date commercially licensed and supported anti malware program that can be remotely managed and updates regularly to protect the health of the endpoint.

4.13 All endpoint computers should have an up to date commercially licensed and supported management agent to facilitate updates, as well as asset and security controls.

4.14 All endpoint computers should be configured to follow industry standard best practices.

4.15 Removable storage devices such as USB drives should be disabled via management agent and only enabled for authorized personnel.

4.16 Internal storage should be encrypted using AES 256 encryption as the minimum level of acceptable key length.

4.17 All machines should be configured with a standard local user account as well as an admin account with an alternate naming convention.

4.18 Standard users should never be granted access to the admin account and their user account should not have admin level rights on assigned systems.

4.19 All system generated accounts should be renamed from the default and deleted or inactivated.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2023	Steven Clymer	Revised

February 2024	Paul Bettinger	Reviewed

2.10.BYOD, Mobile, and Personal Device Policy

1. Overview

The 21st century has seen a dramatic increase in the number of electronic devices that every person owns that can connect to the internet. The rise of cloud-based applications has enabled those many devices to potentially access company data without a direct connection to company networks. The events of 2020 forced everyone to use whatever device was available to them to keep working to support themselves and their organizations. We need to move past the time of expedient action that was required then to a new balanced and secure model moving forward.

2. Purpose

The purpose of this policy is to clearly define how and when a personal or mobile device can be used to access Judge Group systems and data.

3. Scope

This policy applies to all Judge Group staff, contractors, and affiliates.

4. Policy

4.1 The Judge Group does not have, nor does it support a BYOD environment. No personal computer, laptop, IoT device, tablet, or cell phone should be brought into a Judge owned or leased space and connected to the Judge Group internal network.

4.2 Unmanaged devices are only authorized to access guest Wi-Fi services.

4.3 Using a personal computer or laptop to store any Judge Group data is expressly forbidden.

4.4 Through the enterprise license agreement with Microsoft, all employees have access to an O365 E3 license which entitles them to access Microsoft office products via office.com or through installation of office apps on machines.

4.5 Using the Judge Group assigned M3 License for the installation of Microsoft Outlook or OneDrive on a personal computer or laptop is not authorized.

4.6 The use of the browser-based assets of Office.com is the recommended method for Judge Group personnel needing access to office products on a personal computer or laptop.

4.7 Mobile versions of Office products including Outlook and OneDrive are available on Android and IOS devices. In order to access and store email and data on a mobile device it must be enrolled in The Judge Group mobile device management platform.

4.8 The internal storage of the mobile device must be encrypted.

4.9 At a minimum the MDM will be configured to enforce lock screen passwords, screen timeout locks and remote wipe of devices.

4.10 The purpose of the mobile device management platform and encryption requirement are to safeguard both Judge Group and personal data on an employee-owned mobile device.

4.11 To request installation of MDM to enable email and file access on mobile devices staff must contact the IT helpdesk.

4.12 Access to Judge Group email and files on a mobile device is not guaranteed and may be revoked at any time.

4.13 Personal computers and laptops can be used for full remote access utilizing the VMware Horizon agent if the staff role permits.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

Remote Access Policy

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2023	Steven Clymer	Revised
February 2024	Paul Bettinger	Reviewed

2.11.Remote Access Policy

1. Overview

It is no longer possible to have every global employee conduct all business from within the confines of an owned or leased space where the company has built out and controls the network and interconnection resources. It is essential that work conducted outside of controlled networks does not induce unacceptable levels of risk or not comply with other security policies.

2. Purpose

The purpose of this policy is to detail how and when employees may access company resources when not physically operating within a Judge facility to ensure that hose employees do not pose a danger to the company.

3. Scope

This policy applies to all Judge Group staff, contractors and affiliates worldwide.

4. Policy

4.1 All connections to Judge Group networks made from remote non-Judge owned or leased facilities must employ multifactor authentication as part of the authentication process.

4.2 There are only two acceptable methods to connect remotely to Judge resources, via FortiClient VPN or VMware Horizon.

4.3 FortiClient VPN can be used to connect a Judge owned and centrally managed endpoint to resources.

4.4 Username and passwords should not be saved in the VPN client and should manually be entered at each login attempt.

4.5 Personal devices can be used to connect to the VMware Horizon cluster to gain access to a Judge controlled virtual machine to facilitate access to resources.

4.6 Individually assigned company roles determine which if any remote access option is available to an employee.

4.7 Any device attempting to connect to a Judge network can be denied access if the machine does not meet policy standards.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, reporting tools and employee feedback.

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2023	Steven Clymer	Revised
February 2024	Paul Bettinger	Revised Policy 4.2 Vendor

2.12.Audit Policy

1. Overview

The methodical examination and review of an organization's accounts, files, and systems is vital to support the veracity of those items. Without determining truthfulness, one cannot guarantee the confidentiality or integrity of data in those systems, files, and accounts. It is therefore mandatory to audit systems and data on a consistent basis to ensure secure operations.

2. Purpose

This policy provides details concerning the particulars of how and what The Judge Group will audit on a consistent basis to ensure the integrity of data and to uncover any unauthorized access to systems or data.

3. Scope

This policy applies to all endpoints, infrastructure systems, files, applications, databases, and facilities used by The Judge Group or its' subsidiary companies worldwide to conduct any Judge related actions.

4. Policy

4.1 The Judge Group Infosec team shall employ automated tools to assist in auditing, monitoring, and alerting of events such as vulnerabilities, intrusion, and unauthorized access.

4.2 Only the Infosec team is authorized to use scanning tools and protocols on the Judge Group networks. Any use of packet capture or other sniffing utilities must be authorized by the Infosec team and thorough documentation of the intended use must be supplied.

4.3 Log data should be kept for one year if storage space permits. A minimum of 45 days of logs on all infrastructure systems must be available for investigation.

4.4 All data entering or leaving the company networks shall be logged and monitored.

4.5 All logins to switches, routers, and firewalls should be logged and monitored.

4.6 All system and application access shall be logged and monitored. Any suspicious activity should trigger alerts to the Infosec team for investigation.

4.7 Infrastructure systems should be monitored for unauthorized changes from system baselines.

4.8 Changes to file and folder permissions should be logged.

4.9 All changes made to Active Directory will be logged and reviewed.

4.10 Network shares should be scanned for PII to ensure that data is stored appropriately.

4.11 Endpoint devices should be monitored for unauthorized changes from system baselines.

4.12 All user account creation shall be logged and monitored to ensure that all created accounts are valid. If a privileged account is created the Infosec team should be alerted.

4.13 All user accounts will be monitored for changes and any change to a privileged account should trigger an alert to the Infosec team.

4.14 Any account that has its privileges elevated to a privileged level should trigger an alert to the Infosec team.

4.15 All accounts that are deleted should be logged and monitored. If a privileged account is deleted this should trigger an alert to the Infosec team.

4.16 The Judge Group shall contract with an accredited outside third firm to perform external audits as needed to ensure that the organization remains in compliance with best practices and any regulatory obligations.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through, reporting tools and employee feedback.

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2023	Steven Clymer	Revised
February 2024	Paul Bettinger	Reviewed

2.13.Acquisition Assessment Policy

1. Overview

The process of integrating a newly acquired company can have a drastic impact on the security posture of either the parent company or the child company. The network and security infrastructure of both entities may vary greatly, and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

- Assess company's security landscape, posture, and policies
- Protect both The Judge Group and the acquired company from increased security risks
- Educate acquired company about The Judge Group policies and standards
- Adopt and implement Judge Group Security Policies and Standards
- Integrate acquired company
- Continuous monitoring and auditing of the acquisition

2. Purpose

The purpose of this policy is to establish Infosec responsibilities regarding corporate acquisitions and define the minimum-security requirements of an Infosec acquisition assessment.

3. Scope

This policy applies to all companies acquired by The Judge Group and pertains to all systems, networks, laboratories, test equipment, hardware, software, and firmware, owned and/or operated by the acquired company.

4. Policy

4.1 General

Acquisition assessments are conducted to ensure that a company being acquired by The Judge Group does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. The Infosec Team will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Infosec role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to The Judge Group's networks. Below are the minimum requirements that the acquired company must meet before being connected to The Judge Group network.

4.2 Requirements

4.2.1 Hosts

4.2.1.1 All hosts (servers, desktops, laptops) will be replaced or re-imaged with a Judge Group standard image or will be required to adopt the minimum standards for devices.

4.2.1.2 Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by Infosec.

4.2.1.3 All PC based hosts will require Judge Group approved virus protection before the network connection.

4.2.2 Networks

4.2.2.1 All network devices will be replaced or re-imaged with a Judge Group standard image.

4.2.2.2 Wireless network access points will be configured to the Judge Group standard.

4.2.3 Internet

4.2.3.1 All Internet connections will be terminated.

4.2.3.2 When justified by business requirements, air-gapped Internet connections require Infosec review and approval.

4.2.4 Remote Access

4.2.4.1 All remote access connections will be terminated.

4.2.4.2 Remote access to the production network will be provided by The Judge Group

4.2.4.3 In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the Judge Group Chief Information Officer (CIO) must acknowledge and approve of the risk to The Judge Group's networks.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.14.Infrastructure Control Policy

1. Overview

Infrastructure is the broad category of interconnected hardware and software that endpoints connect to in order to request services. At the macro level these interconnected devices span the entire planet and also now reach out into space around Earth. All of this interconnectedness works because of a system of trust between the various systems. At a micro level, all of the patch panels, switches, routers, firewalls, wireless access points, miscellaneous other network devices and servers make up the physical infrastructure. Layered on top all of these physical apparatuses are the software used to control the hardware as well as provide the services and data that endpoints are requesting. Ensuring the security of the micro infrastructure is crucial to maintain the trust that allows our modern interconnected systems to work.

2. Purpose

Protecting the infrastructure to assure confidentiality, integrity, and availability, is the core responsibility of Infosec at both the macro and micro level. This policy outlines what The Judge Group is required to do to participate in the global trust.

3. Scope

This policy applies to all Judge Group infrastructure systems in use worldwide.

4. Policy

4.1 All Judge Group infrastructure systems must synchronize to a central time service.

4.2 The Judge Group IT department is the only authorized group within the company to deploy infrastructure systems that connect either directly or remotely to Judge Group networks. Any violations of this tenet will not be tolerated.

4.3 All hardware and software in use by The Judge Group must be purchased and licensed from the manufacturer or an authorized reseller. Operating gray market systems and software is prohibited.

4.4 All infrastructure systems should be deployed in restricted areas.

4.5 An accurate accounting of infrastructure assets should be maintained and periodically reviewed to assure that all assets are properly tracked. A Configuration management database should be updated to reflect new items, changes to items, as well as removal of deprovisioned systems.

4.6 Systems that have reached end of life and no longer have updates to address vulnerabilities should be removed from production as soon as resources allow.

4.7 Infrastructure systems being removed from service must properly consider the destruction of systems that house data and reduction of environmental impact by supporting responsible recycling efforts.

4.8 All systems should be built from a baseline configuration that follows best practices for the particular type of system and its role within the infrastructure.

4.9 All baseline configurations should be recorded in the CMDB.

4.10 Changes to system configurations should be managed through a well-defined change control process. Change control drives better results, helps create understanding of the rate of change, helps mitigate bad changes, and improves consistency and efficiency in managing infrastructure.

4.11 All systems should have an identified primary custodian responsible for the health and operation of the system. Although there may be shared custodial control of a system the primary custodian would be relied on in the event of an incident. Should an incident with a system arise the custodian must report this to Infosec as quickly as possible.

4.12 Groups of infrastructure items such as firewalls, switches, printers, applications servers should be configured for centralized management whenever feasible.

4.13 A centralized anti malware service that is routinely monitored and updated should be used to protect Windows and Linux based servers across the infrastructure.

4.14 System event and security logging should be enabled on all systems. A minimum of 45 days' worth of logs should be maintained but if space permits logs should be retained for 1 year.

4.15 Systems should be configured to send logs to a centralized logging service for automated analyzation.

4.16 All system drives and databases should be encrypted using a commercially supported product with a minimum requirement of AES with 256bit encryption key.

4.17 Systems that come pre-configured with default accounts should have those accounts renamed disabled and deleted if possible.

4.18 All passwords used for infrastructure systems must conform to the Password Policy.

4.19 The practice of least privilege should be adhered to so non elevated accounts should be used on systems unless the action at hand requires elevated privilege to complete.

4.20 Multi factor authentication should be used to connect to all infrastructure systems.

4.21 Only secure channels such as SSH should be used to connect to infrastructure systems and non-secure connections such as HTTP, FTP, Telnet should be disabled wherever possible.

4.22 Unused system services should be disabled wherever possible.

4.23 Only in use ports should be accessible all other ports should be set to admin disabled.

4.24 TLS version 1.2 or higher should be used for all network communications between systems.

4.25 Systems should be routinely monitored for security vulnerabilities and patches tested and applied in a timely fashion.

4.26 Systems should be backed up daily and at least one complete copy of backups should be store offsite with no direct connection between the storage and the Judge Group network.

4.27 Critical physical hardware should be operated in a redundant capacity in case of failure.

4.28 All branch infrastructure systems should have adequate surge protection and have a minimum of 15 minutes of battery power to carry them through a short disruption of power.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

Infrastructure systems refers to any server, host, hypervisor management system, remote access card, switch, router, firewall, network multi-function device, storage area network, network attached storage and any other device that provides services to groups of people in an interconnected environment.

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.15.Incident Response Policy

1. Overview

Things will happen. Incidents can come in many forms and have varied effects on an organization. Having a plan before something bad happens greatly increases the chance of a less negative outcome.

2. Purpose

Due to the varied nature of the almost countless incidents that are possible, this policy is meant to be a guide to The Judge Group and the Infosec team on how to prepare for and respond to security related matters in a general sense. Unlike other policies, the Incident response needs to be flexible to face the ever-changing threat landscape.

3. Scope

This policy applies to all Judge Group systems, data, networks, as well as any person or device accessing those systems and data.

4. Policy

4.1 The Judge Group takes the potential threats to the safety of its staff and property very seriously. Likewise, protecting the confidentiality, integrity, and availability of systems and data is vital to the continued operation and reputation of the organization.

4.2 All members of the Infosec team should be well versed in the details of NIST SP800-61r2 as emulating an incident response as detailed in that publication would satisfy the actions of a prudent man.

4.3 The Judge Group security team operates with limited resources and as such must strike a balance between vigilance and alarm. To that end, information security efforts should be focused nominally on events and primarily on incidents.

4.4 **Events** are to be categorized as an exception to the normal operation of Judge Group facilities, infrastructure systems, or services. Events are reported through tickets or phone calls to the helpdesk, or through monitoring performed by automated systems. It is the responsibility of the IT Services team to make Infosec aware of events that come to them that may require Infosec scrutiny.

4.5 **Any Judge Group staff or affiliate who witnesses or who is party to an event must report the event to the IT helpdesk immediately**.

4.6 Not all events will become incidents.

4.7 **Incidents** are events that have been assessed by the Infosec team and found to violate Judge Group Information Security Policies or threaten the confidentiality, integrity, or availability of Judge Group systems or data.

4.8 In order to promote consistency and clarity, incidents shall be rated as other risk factors using the catastrophic, severe, moderate, minor, and negligible level rating.

4.9 Assigning severity levels also aids the team in assigning resources properly in the event of multiple incidents occurring simultaneously.

4.10 Although the Infosec team should be able to handle minor incidents by its own means, incidents of moderate through catastrophic level will require the activation of an Incident response team to handle the most potent incidents that could arise.

4.11 The incident response team should be comprised of the Infosec team as well as the IT Leadership team. The inclusion of the IT leadership team facilitates a couple of important items. Based upon the nature of the incident, the Leadership team can assign their most qualified technologists with expertise in the area affected by the incident. Including the ITLT also ensures that the entire department is aware that ongoing projects could be impacted or completely halted by a needed emergency response.

4.12 If an incident rises to the level of activating the IRT then senior management should formally be advised that an incident is occurring so they can take appropriate steps as needed.

4.13 All Judge Group staff must cooperate with the incident response team while they work towards resolution of the incident affecting the company. Depending on the severity and type of incident senior management should support the IRT by honoring requests for staff assistance from other groups with expertise related to the incident.

4.14 Based on NIST SP 800-61 documentation every incident has a lifecycle. The life cycle consists of Preparation, Detection & Analysis, Containment, Eradication & Recovery, and finally Post-Incident Activity.

4.15 The Judge Group Infosec team's daily operations reside within the incident life cycle and requires them to maintain a level high level of focus to remain effective.

4.16 **Preparation:** The following actions are undertaken to reduce the occurrence of incidents and ensure that The Judge Group can respond to an incident in an effective manner.

- The Judge Group periodically performs risk assessments of systems, applications, and processes so that the company can mitigate threats and vulnerabilities thereby reducing risk to an acceptable level. Risk assessments are performed both internally and externally via a third-party security firm.
- Infrastructure systems and endpoints are configured via standard configurations. Systems and endpoints have both a management agent to facilitate auditing of configurations and application of patches on a scheduled basis as well as centralized anti-malware to protect and detect potential malicious activity. In the virtualized system environment security services and anti-malware is deployed at the host level to protect the entire environment.
- Network security is facilitated through central management of NGFWs, centralized analyzation of traffic logs, segmentation, and restriction of cross network traffic. The standard network rule is an implicit deny and only explicitly allowed traffic can traverse the network. We utilize a SIEM tool to analyze network traffic, monitor behavior, and help us respond to incidents on the network.
- User Awareness and Training is essential in reducing the number of incidents. The Judge Group operates an LMS to provide training to staff and contractors. The LMS host modules specific to end user security practices. We run monthly phishing awareness campaigns and coach staff where needed. In addition, we post security related items in social postings as well as notices concerning security topics.
- An action and contact list is maintained for incident notification for the ITLT and senior management.

4.17 **Detection and Analysis:** Although it is impossible to account for all possible incidents The Judge Group is committed to maintaining a system and approach to detect and mitigate incidents that use common attack vectors.

- **If an incident occurs with the potential for loss of life contact authorities immediately and try to reduce the loss of life by any means possible.**
- Incidents arising from malware on removable media is mitigated by disabling USB mass media support via the installed management agent.
- Enforcing failed login attempt lockout rules and CAPTCHA on web site forms helps to detect and mitigate attrition incidents
- Email is the most common attack vector, and The Judge Group leverages Proofpoint to detect, analyze, mitigate, and provide awareness tools to users to protect what is still the primary means of cross company communication.
- Our NGFWs employ web reputation services to analyze web requests to detect malicious site and block access to them reducing the number of incidents involving compromised or malicious sites.
- Improper usage of company assets and loss or theft of that equipment are important vectors to monitor for security incidents. The Judge Group uses tools to monitor normal behavior so that the Infosec team can be alerted to non-typical behaviors. Users do not have admin access to their machines to mitigate installation of malicious software. The IT department manages and tracks assets as well as having remote access to machines to deny user access should the need arise.
- Although there are other avenues for malicious incidents to occur, The Judge Group maintains a suite of tools to automatically monitor activities and employs staff to actively review daily events so that there is a baseline of what “normal” activity represents. This collection of data allows the Infosec team to analyze events to detect abnormalities and then react.

4.18 **Containment, Eradication, and Recovery:** Once there has been a determination that an incident is in progress, evidence quickly needs to be gathered so that a course of action to contain, remove, and then ultimately recover from the incident, can be found. Once again, the variables are innumerable so having some general response framework will be critical in the success of this phase of the lifecycle.

- The IRT should play to the strengths of its members and split the functions of the group into, analyze and investigate, fix and remediate, and communicate and annotate.
- In order to properly proceed towards containing the occurring incident it should be classified into a category so that correct actions can be undertaken. A grease fire is a good example of classification of an incident as just a fire is not enough. Water is the go-to control to contain fire but in the case of grease it is a detriment. The Infosec team should devise an operational category assignment to help increase response time for particular known incident types.

- Once the incident has been classified the IRT should take steps to triage systems to prevent the spread of the incident before it can cause more damage.
- Triage measures must be conducted with due care to ensure that all possible evidence can be collect from affected systems.
- Successful triage activities include, finding all affected systems and isolating them or mitigating what has happened to them, if the incident involves a breach from the outside, then cutting access and determining what systems or data are affected, if it is an internal use incident cutting access to the user and determining the damage done by the user. There are many other items, but this should present the general goal of triage.
- Once triage efforts have taken place there should be enough information to properly communicate to those outside the IRT what has happened, and then next steps can be determined.
- Evidence should be collected and maintained. All evidence needs to be logged, securely stored and a complete chain of custody must be maintained.
- Once the incident has been contained and the full extent of the incident has been determined, removal of the problem and remediation of systems can begin. Depending on the breadth of the incident prioritization of what systems should be remediated first should be determined. A hierarchy of systems should be maintained to assist in the prioritization of system remediation.

4.19 **Post-Incident Activity:** No system is perfect, with the ever-evolving threat landscape incidents both large and small will happen. As recovery concludes and the incident is wrapping up meetings need to be held to determine how we can improve response the next time an incident occurs. Some items of note for these proceedings are.

- A timetable of events should be constructed so that the incident can be tracked backwards to the source.
- If the incident caused machines to go offline were the recovery times acceptable?
- Did pre-existing procedures provide adequate methods to react and recover from the incident?
- How well were communications handled?
- Do we know what controls need to be implemented to stop this from happening again?
- Were the skills of the team adequate or do we need training and or outside help if such an incident occurs in the future.
- How could we have reacted differently to get a better outcome?
- Are existing tools enough or do we need to investigate other options to better detect analyze and mitigate such incidents in the future?
- Finally, a report of the incident should be created and retained for the record.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2022	Steven Clymer	Initial Release
February 2024	Paul Bettinger	Reviewed

2.16. Disaster Recovery Policy

1. Overview

Disasters do not happen every day, at least we hope that they do not. It is difficult to devote resources to something that may never happen when there is always so much to do today. Restoring business operations after a natural or man-made disruption can only happen if there is a tested disaster recovery plan that the company can follow to become functional again.

2. Purpose

The purpose of the disaster recover policy is to provide general rules for the creation, implementation, and management, of The Judge Group disaster recovery plan.

3. Scope

This policy applies to Judge Group employees accountable for ensuring a recovery plan is developed, tested, and maintained.

4. Policy

4.1 The judge Group must create and implement a business continuity and disaster recovery process plan.

4.2 The DR plan must be periodically tested, and the results should be used for the ongoing improvement of the plan.

4.3 The DR plan, at a minimum, will identify and protect against risks to critical systems and sensitive information in the event of a disaster.

4.4 The DR plan shall provide for contingencies to restore information and systems if a disaster occurs. The core goal of the disaster recovery plan is to restore normal business operations with a RPO of 30 minutes and RTO of 24 hours.

4.5 While planning the DR strategy the management team should devise a pre-arranged order of succession to remove ambiguity of authority should the disaster result in loss of life of key personnel.

4.6 Detailed documentation of the DR plan should provide clear instruction on all procedures associated with restoration of systems so that unfamiliar technical staff could follow the plan to successful completion.

4.7 Multiple copies of the DR plan should be stored in geographically diverse locations.

4.8 Scenarios based on different types of disaster should be devised to improve response times and resource allocation.

4.9 The increased cost of multiple off-site backups should be approved and maintained.

4.10 Staff should be trained to execute the recovery plan and testing of the plan should be done at least annually. The testing and training should involve alternates to the primary staff to increase resilience.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance through various methods, including but not limited to, periodic walk-through

5.2 Exceptions

Any exception to this policy must be approved in advance by the Infosec team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
March 2023	Steven Clymer	Revised
February 2024	Paul Bettinger	Reviewed

2.17.Breach Response Policy

1. Overview

A data breach is a specific type of incident where information is stolen or taken from a system without authorization or knowledge of the owner. Companies that suffer data breaches incur both financial and reputational consequences based upon the breach itself and their conduct after the discovery of a breach.

2. Purpose

The purpose of the Breach Response policy is to supply The Judge Group with a reaction plan in the event of a data breach.

3. Scope

This policy applies to Judge Group Privacy Officer, Infosec team, Incident Response Team, Judge Legal department, and Senior Management.

4. Policy

4.1 Any Judge Group staff or affiliate who suspects a data breach to have taken place must contact the IT helpdesk immediately to report the incident.

4.2 The Incident Response Plan should address the technical portions of the incident while this policy concerns the governance and communications surrounding the data breach.

4.3 Once the nature and the breadth of the breach has been quantified the Privacy Officer, ISO, CIO, and Senior Management should be provided with an initial report of the who, what, where, when, and how of the incident.

4.4 A risk assessment of the initial report should be conducted to quantify the specific amount and data type that was compromised.

4.5 The legal department and senior management must determine if law enforcement or other outside parties need to be notified and coordinate with the marketing team on the content of the communications.

4.6 In the interest of our valued clients, we will strive to inform clients within 30 days of a discovered breach.

4.7 If the data breach involves health related information the legal department should review https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html to see if the provisions apply.

4.8 If a data breach occurred and Social Security Numbers were involved the legal department should work with the marketing team to contact the major credit bureaus.

4.9 Notification timing with regards to data breaches are important as various local, state, federal, and client contracts dictate when notice of a breach must be sent. The Judge Group legal department should respond according to requirements.

4.10 Should a determination be made, that notice must go out to individuals then the following information should be included in the notification.

- How the breach happened
- What information was taken
- How the stolen information has been used
- What actions have been taken to remedy the situation
- What actions are being taken to protect those affected
- How to reach contacts for further discourse

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, tool reports, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.18.Secure Software Development Policy

1. Overview

Web apps, micro apps, software suites, operating systems, the myriad of different applications created to provide functionality to the masses take time and money to produce and building security into applications garners no money for the effort, so it often becomes an afterthought if anything. Designing software with security in mind from the start is more important than ever as software becomes a ubiquitous part of modern existence.

2. Purpose

The purpose of this policy is to provide a general framework for Judge Group developers to be able to weave security practices into their processes from the beginning of software development to reduce the potential number of vulnerabilities in the products they produce.

3. Scope

This policy applies to all Judge Group staff involved in application development.

4. Policy

4.1 The Judge Group must ensure that applications it develops in house follow an SDLC process which is consistent, repeatable, and factors in security at every stage.

4.2 A robust change control methodology must be in place that can be audited by the Infosec team or Senior management on a periodic basis.

4.3 Code changes should be reviewed by qualified personnel other than the author prior to release.

4.3 Production, test, and development activity should be logically or physically separated from one another to ensure security of production systems.

4.4 Active production environments should not be re-used as test environments unless all production data has been removed.

4.5 Production data should not be used in in testing or development environments. Should production data need to be used in a test environment that use must be authorized ahead of time by the CIO.

4.6 Source code and system backups should be stored in an offsite location.

4.7 Applications should be tested against the criteria listed in the OWASP testing project. The current iteration can be found at https://owasp.org/www-project-web-security-testing-guide/v41/

4.8 Automated vulnerability testing tools should be leveraged to test applications prior to deployment.

4.9 Software developers should attend yearly classes devoted to software security to stay abreast of changes in the threat landscape.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, tool reports, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.19. Training and Awareness Policy

1. Overview

People are the most valuable asset of any organization, but they also represent the greatest threat to the security of an organization. In order to reduce the risk imposed by its' people to the confidentiality, integrity, and availability of company systems and data, a formal program to train and make people aware of good security habits is needed.

2. Purpose

The purpose of this policy is to provide an outline of what The Judge Group security and awareness efforts should strive to accomplish.

3. Scope

This policy applies to Judge Group employees and contractors.

4. Policy

4.1 Educating all Judge Group staff and contractors about their security responsibilities is important to the continued success and positive reputation of The Judge Group.

4.2 The Judge Group security policies are posted so that all staff can review and understand them.

4.3 Because it is necessary to train staff and contractors The Judge Group operates a LMS to increase knowledge with specific modules tailored for information security topics.

4.4 All employees are required to complete cyber awareness training within their first 30 days of employment.

4.5 Each year all employees are required to review security specific policy information and acknowledge that they understand and will comply with those policies.

4.6 The Infosec team operates email phishing campaigns to promote awareness of this common threat.

4.7 Periodically the Infosec team will publish security related articles and information to increase awareness of security related topics.

4.8 The training and awareness efforts are reviewed and adjusted yearly to reflect changing security variables.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, tool reports, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

7. Definitions and Terms

8. Revision History

Date of Change	Responsible	Summary of Change
February 2024	Paul Bettinger	Reviewed

2.20.Data Retention and Classification Policy

1. Overview

After people, company data is the most important asset that needs to be protected. Unlike people, data has no long-term intrinsic value and should be destroyed once it no longer has any value to the company.

2. Purpose

The purpose of this policy is to outline the length of time that particular types of data hold value to the company and define how data should be handled when retention periods expire.

3. Scope

This policy applies to all data owned and stored within Judge Group internal systems and on external systems and services leased by The Judge Group.

4. Policy

4.1 All data controlled by the enterprise should be classified by category, sensitivity, and criticality.

4.2 Information criticality refers to how important that data is to function of the enterprise and should be rated on a 4-point tiered scale of 1 being critical to the function of the company and 4 being of no consequence.

4.3 Information sensitivity is currently assessed to be confidential, restricted, or public and is a measure of potential impact the data could have if unauthorized persons are able to access a particular data set.

4.4 Categories of data are tags to identify custodian, group, department, or other criteria deemed useful to prescribe what retention periods should be applied to specific data sets.

4.5 Retention periods are the length of time particular data should be retained by the enterprise before being destroyed and these values are influenced by legal, regulatory, and business needs.

4.6 **All data should be prescribed a retention period.**

4.7 Due to cost and system constraints some data may be archived during the lifecycle which may increase the time required to view such data, but archived data is still subject to retention periods and does not imply that the data will be available in perpetuity.

4.8 The chart below contains data categories and retention periods for those particular types of data.

Department	**Category**	**Retention Period**
Administration		
	Departmental Documents	6yrs
	Internal Services	3yrs
	Records Destruction Certs	10yrs
	ReferenceMaterials	3yrs
	Contracts after term is ended	5yrs
Audit		
	External Financial Audits	10yrs
	External IT Audits	5yrs
	Internal Financial Audits	3yrs
	Internal IT Audits	3yrs
	SOX Compliance	7yrs
	Training and Certification Records	3yrs
Finance		
	Acquisition and Divestment	10yrs
	Bank Account Info	6yrs
	Budgets and Forcasts	3yrs
	Strategic Planning	6yrs
	Financial Statements	10yrs
General Data not covered under departments	Email	5yrs
	Personal Documents	4yrs
	Teams Chats	3yrs
	Teams Files	4yrs
	File Server Files	4yrs
	One Drive Files	3yrs
	Share File Files	5yrs
	Share Point	3yrs
	Onbase Files	6yrs
Human Resources		
	Benefit Enrollment Information	6yrs
	Benefit Plan Adminstration	6yrs
	Compensation Planning	6yrs
	Employee Counseling	3yrs post seperation
	Equal Employment Opportunity	6yrs
	Employee Recuitment	3yrs
	Training and Devlopment	3yrs
	Healthcare Data	No less then 5yrs

4.9 Any data that falls into multiple categories should be retained for whatever the longest retention plan calls for.

4.10 All healthcare data shall be retained for a period of not less than five (5) years and shall be immediately available to the governmental or administrative agency seeking such data.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team verify compliance to this policy through various methods, including but not limited to, tool reports, direct monitoring, and feedback from staff.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, including termination or legal prosecution.

6. Related Standards, Policies and Processes

7. Definitions and Terms

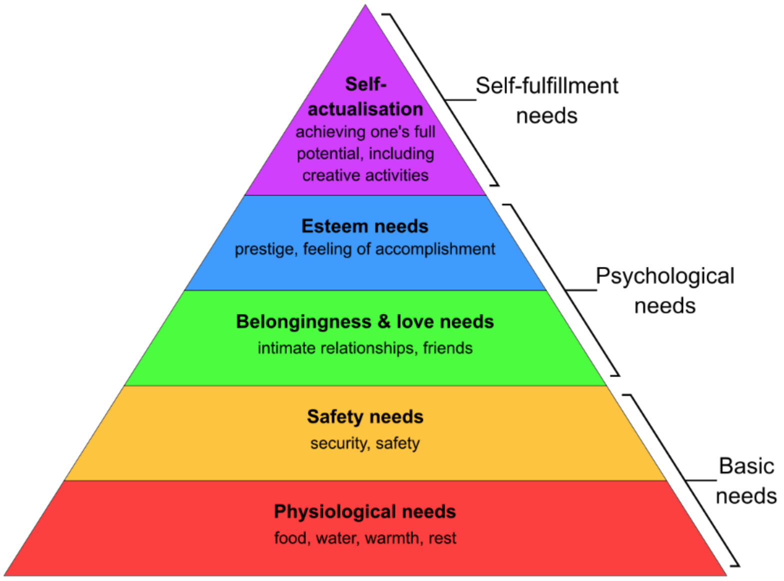
8. Revision History

Date of Change	Responsible	Summary of Change
March 2022	Steven Clymer	Initial Release
February 2024	Paul Bettinger	Adjusted policy 4.8

3. Appendices

A. Maslow's Hierarchy of Needs.

1.


Self-actualisation
achieving one's full potential, including creative activities
Esteem needs
prestige, feeling of accomplishment
Belongingness & love needs
intimate relationships, friends
Safety needs
security, safety
Physiological needs
food, water, warmth, rest
Self-fulfillment needs
Psychological needs
Basic needs

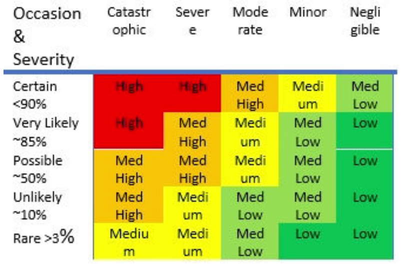
B. Risk Assessment Process

There are many methodologies that can be used to perform risk assessments. The Judge Group risk process is based on NIST SP 800-30 and is geared towards a quantitative approach in lieu of a qualitative one. The below defined sequence of action is not meant to be linear and some of the actions may occur simultaneously.

- **Assessment Target**: Define the scope for the assessment. An assessment can be aimed at a single system or process, or it can be a broad topic such as the risk of fire burning down a datacenter. Information must be gathered or provided so that a definitive boundary of what is and what is not part of the assessment so that a clear understanding can be reached.
- **Risk Variables**: A thorough and objective calculation of potential risk sources for the given target of assessment should be identified. There are many types of risk and NIST SP 800-30 contains a useful list of risk threats for IT related systems. The goal here is to come up with a list of threat sources that could exploit vulnerabilities.
- **Identify Weaknesses**: No system or process is perfect. Examine the target and come up with a list of factors that a risk source could potentially expose and or exploit.
- **Mitigation Analysis**: What controls are, will be, or can be put into place to reduce the impact of a realized risk or reduce the likelihood of a threat realization.
- **Rate of Occurrence**: How likely or how often can the identified risk sources be expected to happen given the controls and safeguards in place. It is important to

quantify this, and we use a scale based on times per year that a risk may manifest itself.

- **Severity Level**: For each identified risk we determine how much impact that risk would inflict to the company based on associated costs of the assessment target.
- **Risk Determination**: By cross referencing the Rate of Occurrence and the Severity Level we can come up with an overall risk rating so that senior management can decide how they wish to respond to the risk.



Occasion & Severity	Catastrophic	Severe	Moderate	Minor	Negligible
Certain <90%	High	High	Med High	Medium	Med Low
Very Likely ~85%	High	Med High	Medium	Med Low	Low
Possible ~50%	Med High	Med High	Medium	Med Low	Low
Unlikely ~10%	Med High	Medium	Med Low	Med Low	Low
Rare >3%	Medium	Medium	Med Low	Low	Low

- **Recommendations**: The risk assessor should take due care and investigate if there are other controls that could be employed to reduce the risk to an acceptable level.
- **Documentation:** The collected information is documented in an official risk report with recommendations for senior management to accept, avoid, reduce, or transfer the risks that have been identified.

After all of these steps have been undertaken senior management should sign off on the documentation and clearly define what actions should be undertaken next. If reduction is the chosen option, then evaluating prioritizing and implementing the recommended controls should commence. Risk must never be ignored. Once a report is prepared senior management has a responsibility to respond to the risk. Sometimes even great risks must be accepted because of monetary or situational realities. Acknowledging such risks is still important from a process and governance perspective.