TEKsystems Own change | Global Services

New Hire Documentation Checklist (For TGS HR use only)

EID	Name	DOJ	Employment Type

Documents	Remarks
Employment Documents	
Passport Size Photograph	
BGV Application Form	
Export Control Questionnaire	
Information Security Onboarding Addendum	
Information Security Policy Acknowledgement Form	
Non-Disclosure Agreement	
Acceptable Use Policy	
Drug Policy	
IT Policy (Contractors and Interns)	
PF Form: Form 11/ Form 2/ Form 26(6) ASI	
Gratuity Form	
Resume	
Interview Assessment Form	
Candidate Particular Form	
TEK Offer Letter /Appointment Letter	
Previous Employer (s) Relieving Letter (7 years)	
Previous Employer Salary Slips (3 months)	
Educational Documents	
10th	
12th	
Graduation (Consolidated or Semester Mark sheets)	
Post-Graduation (Consolidated or Semester Mark sheets)	
Special Qualification	
KYC Documents	
Passport*	
Aadhaar Card*	
Voter ID	
Birth Certificate	
PAN Card*	

Received & Verified by **TEK Representative Signature**

TEKsystems Own change | Global Services

Information Security Onboarding Addendum – Global Services

Date: 10/feb/2023

I Harshit Mishra a TEKsystems Global Services employee currently assigned to its Customer, hereby acknowledge that I have spoken to my local market TGS Representative, _____, (the "Representative") regarding the Customer and TEKsystems Information Security Policies. During this discussion, the Representative and I discussed the awareness, importance, and reinforcement of both Customer and TEKsystems Information Security Policies.

As an initial matter, the Representative reminded me that Customer is monitoring my activities while assigned as a TEKsystems employee to ensure compliance with the respective Information Security policies.

In that regard, the Representative and I specifically discussed the following:

- The prohibition regarding the downloading or transferring of ANY data or files to an external device or email without, prior, written consent of Customer.
- The prohibition regarding the use of a file sharing service or cloud based service such as GitHub or Drop Box or posting any data to any external site.
- The importance of recognizing that any data or information provided to me or to which I have access to or actually access while assigned to Customer is not only intellectual property of Customer but also confidential and proprietary data of Customer (the "Data"), and that at no time shall I disclose the Data.
- The criticality of ensuring that Protected Health Information ("PHI"), Personally Identifiable Information ("PII") or Intellectual Property ("IP") is kept confidential and handled in a manner consistent with Customer standards.
- The requirement to periodically review the Information Security Training provided to me byTEKsystems to ensure Information Security compliance.
- If any request is made of me to deviate from either or both Customers' or TEKsystems' Information Security Policy, that I will immediately contact my Representative.

Additionally, I will take all measures to prevent any of the following actions which could lead to a potential Information Security breach:

- Loss or theft of a customer or TEKsystems issued device / laptop containing customer information
- Unauthorized download, transmission, use / access or disclosure of customer information
- Insertion of malicious software on Customer's system
- Any loss or theft of a customer-provided ID/security badge, key, password token, access credentials or key card

Signature: Harshit

Finally, my Representative and I discussed the additional following measures I will follow:

- Ensure use of only Customer-authorized devices and networks
- Obtain Customer's prior, written authorization before saving ANY information to a portable device (*e.g., USB drive*, CD, iPod, iPad, mobile phone) and/or removing that device from the Customer premises. Ensure that workstations and authorized portable storage devices are locked at all times when I am away from my *work* station.

Sincerely,

TGS HR Representative: _____
(Signature)

ACKNOWLEDGED:

Harshit Mishra
(Employee Name)

Harshit
(Signature)

TEKsystems Own change | Global Services

Information Security Program Policies Acknowledgement Form

TEKsystems is committed to ensuring safety, security and privacy of personal, protected and other Company data in adherence with applicable data protection and data privacy laws. Accordingly, the Company has established the Information Security Program (the "Program") which encompasses several related Program policies which are designed to address compliance with these requirements.

I understand that revisions to the Program policies may occur and that all such revisions or changes will be communicated through Company corporate notices to all employees. I further understand that revised Program policies will supersede, modify, or eliminate existing Program policies. Only the Allegis Information Security Council, TEKsystems' parent company, has the authority to adopt any revisions to the Program policies.

By signing below, I understand that I am acknowledging that I have received the Program policies and that I understand that it is my responsibility to read and comply with the Program policies and any subsequent revisions made to the Program policies. Finally, I agree to notify the persons listed below if in the event of an issue including an information security breach related issue I am involved in or become aware of as a result of my employment with TEKsystems.

Harshit

Employee's Signature

Harshit Mishra

Employee's Name

10/feb/2023

Date

NOTICE

In the event of any Information Security matter or incident, contact:

Primary Contact:
TEKsystems Information Security Officer
infosecofficer@teksystems.com

Secondary Contact:
TEKsystems Privacy Officer
privacyofficer@teksystems.com

Non-disclosure and intellectual property assignment agreement with Allegis Services (India) Private Limited ("TEKsystems Global Services")

I, Harshit Mishra son/ daughter of Pankaj Mishra, of Allegis Services (India) Private Limited,[TEKsystems Global Services] Arliga Ecoworld Infrastructure Private Limited, 801, 8B, 8th Floor, Bellandur, Bengaluru, Karnataka 560103 and residing at 105/1a,Gandhi Gram ,Kanpur and having permanent address at 105/1a,Gandhi Gram ,Kanpur ("you") agrees as follows:

Whereas, during the course of your employment and service with Allegis Services [TEKsystems Global Services Pvt Ltd] ('Employer') you will be providing certain services for TEKsystems Global services customers as per the services agreement entered into between your Employer and Customer ('Services'), and you hereby agree that you may during your involvement in the Services come in contact with the Confidential Information (as defined below) of Customer, or its clients, Staffing Agencies or vendors ('Information').

1. You agree:

(a) to hold the Information in complete confidence and, unless you have Customer's prior written consent, not disclose it, in whole or in part, to any person other than those directly concerned with the Services and whose knowledge of such Information is essential for such purposes;

(b) not to use the Information for any purpose other than to enable you to perform the Services unless you have Customer's prior written consent;

(c) to return to Customer upon demand any and all Information, written documents (or copies thereof) equipment, computer software or other materials entrusted to you in the course of the performance of the Services and not to distribute in whole or in part any such documents, materials or other items without Customer's prior written consent; and

(d) to comply with all procedures and policies specified by Customer from time to time including but not limited to Physical Security, Data Security or Information Security.

2. No announcement or disclosure of the Services performed by you is permitted without the prior written consent of Customer.

3. The confidentiality obligations in this Agreement shall be binding on you for so long as the Information retains commercial value which may be even after you cease performing the Services.

Signature: Harshit

The intellectual property related clauses given below shall last for the duration of any related Intellectual Property Rights.

4. You agree that during the Services being provided by you, you might develop or be involved in certain processes, software, products, services or any other materials for Customer or Customer's clients. You agree that all rights including any Intellectual Property rights in any material developed or used by you during your provision of Services to Customer shall be the property of Customer, you hereby irrevocably and unconditionally assign all rights including ownership rights or Intellectual Property rights in such materials to Customer or such other party as may be specified by Customer. You agree that you will assist Customer, or any other party assigned by Customer in documenting or filing for any registrations in order to protect Customer's rights in such Intellectual Property Rights.

5. You hereby agree that any breach by you of the obligations specified herein, will lead to severe losses for Customer or its clients and hence you agree that Customer or another party specified by Customer may take legal action against you in the event of such breach, such legal action may include but not be limited to injunctive or equitable remedies or actions for specific performance in the relevant court of law.

6. You agree that this agreement shall be governed by Indian law and consent to the jurisdiction of the federal and state courts of Bangalore, India.

Employee full Name: Harshit Mishra

Signature: Harshit

Place: Bangalore

Date: 10/feb/2023

ALLEGIS GROUP

Opportunity Starts Here.

Information Security Policies Framework

Acceptable Use of Electronic Resources Policy

Document ID:	AG-ISMS-POL-ERP
Version Number:	12.0
Issue Date:	01, January, 2023
Next Review:	01, January, 2024

THE OFFICIAL VERSION OF THIS DOCUMENT WILL BE MAINTAINED ON-LINE. BEFORE REFERRING TO ANY PRINTED COPIES PLEASE ENSURE THAT THEY ARE UP-TO-DATE.

CONFIDENTIAL

Date: 10/feb/2023 Signature: Harshit

1 CONTENTS

Date: 10/feb/2023 Signature: Harshit

Date: 10/feb/2023 Signature: Harshit

1 INTRODUCTION

This Acceptable Use of Electronic Resources Policy (the "Policy") is part of the Information Security Policies Framework and sets out important rules governing the use of Electronic Resources and Social Media, including the use of any of these on personal accounts through personal equipment or through other non-Company assets that connect to any Company network or affect the Company in any way, whether intentional or not.

This Policy reflects the state of technology as of the date of its adoption; therefore, technological developments may exceed the literal text of this Policy.

This Policy also outlines the use of external or cloud services such as Dropbox, Gmail and Google Docs, Box.com, Salesforce, Amazon Web Services, and Azure.

The Company entity that is legally responsible for the processing of any Personal Data processed about you for the purposes of this Policy is the Company entity that employs or contracts with you.

2 INCIDENT REPORTING

It is important to the Company that it is aware of incidents and violations related to this Policy so that it can appropriately address them, so the Company needs your help in identifying those incidents and violations. You must report incidents and violations related to this Policy as follows:

- Online at https://infosec.allegisgroup.com (preferred method) **OR**
- By telephone at +1-866-483-5411

With regards to incidents and violations of this Policy:

- All incidents and violations of this Policy must be reported immediately;
- If you report an incident or a violation of this Policy, then you will be expected to cooperate in the investigation; and
- Retaliation towards those who report incidents and violations of this Policy in good faith is a serious violation of this Policy and must be reported immediately.

3 DEFINITIONS

The terms defined in this section, shall for all purposes of this Policy, have the meanings specified as follows:

(1) "**Company"** means Allegis Group, Inc. and its subsidiaries worldwide. In this Policy, Company is also referred to as "we" or "We" or "us" or "Us".

(2) "**Company Personnel**" means all Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents and also other third parties such as partners, customers and suppliers who work with the Company's information assets and/or Personal Data (for example payroll providers, benefits providers, auditors, lawyers) who have access to the Company's systems or information. In this Policy, Company Personnel is also referred to as "You" or "you" or "Your" or "your".

Date: 10/feb/2023 Signature: Harshit

(3) "**Electronic Resources**" means any (a) information technology equipment, devices or related equipment (such as computers, laptops, desk phones, mobile phones, tablet PCs (e.g., iPad), thumb drives or other storage devices or multi-function printer/copier/scanner/fax machines); (b) electronic key fobs/cards; (c) internet and internet connections; (d) intranets; (e) network file shares (such as the Q:, S:, T:, U: or O: drives); (f) file sharing sites (such as Team Sites and SharePoint); (g) databases; (h) online subscriptions and services (such as WebEx); (i) applications, whether cloud or on-premise (such as Office 365, voice mail or Connected); (j) wearable or 'nearable' devices or any equipment comprising the 'internet of things', and (K) CCTV and any other similar resources of any kind which are (i) supplied by the Company to you for use for work-related purposes or (ii) not supplied by the Company to you, but are either: (a) used by you to connect to any Company network or (b) used in a way that affects the Company, whether intended or not.

(4) "**EU Sensitive Personal Data**" means information collected from individuals from the EU (collectively the "EU" for purposes of this Policy refers to the EEA countries, the UK and Switzerland) relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, as well as data concerning health or data concerning a person's, sex life or sexual orientation. In some EU member states, it may also include information about a person's criminal convictions.

(5) "**Information Security Policies Framework**" means this Policy and all other policies that state they are part of the Information Security Policies Framework, including any supplements and/or procedures related to those policies.

(6) "**Personal Data**" means any information that relates to an identifiable individual as defined in applicable data protection laws (as they may be amended from time to time).

(7) "**Sensitive Personal Data**" means collectively EU Sensitive Personal Data, any type of Personal Data that is considered "sensitive" data under applicable data protection law and for all individuals, includes health data, biometric data, genetic data, an individual's account log-in, financial account, debit card, or credit card number when in combination with any required security or access code, password, or credentials allowing access to an account, and social security numbers, driver's license numbers, or other state/national identification numbers and state/national identity documentation (such as passports).

(8) "**Social Media**" means collectively forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as photos or videos), and without meaning to create an all-inclusive list, includes any of the following: Facebook, LinkedIn, Twitter, TikTok, Pinterest, Instagram, YouTube, WeChat, WhatsApp, Snapchat, Tumblr, Reddit, Quora and Flickr and Company-maintained sites (such as Yammer, Chatter and Microsoft Teams chat).

4 SCOPE

The target audience of this Policy is Company Personnel. Any Company Personnel must follow this Policy where they operate at a Company facility or when accessing any Company systems or networks (including, for example, when working from home or other remote locations). Any Company Personnel who are operating at a third-party site that is not controlled by the Company (for example a Company client site) may be subject to any additional policies provided to the Company Personnel by that third party. Any Company Personnel who are operating independently of the Company and are not physically present at a Company worksite or accessing Company systems or networks may, as a

Date: 10/feb/2023 Signature: Harshit

default, follow this Policy or may provide their own Policy, as long as such Policy is no less rigorous than this Policy.

This Policy applies to all Company information and data, whether or not the activities involving Company's informational assets are conducted from the Company's premises or on Company-owned equipment.

This Policy establishes baseline requirements, with the option of stricter local or regional policies subject to written approval from the Information Security Office. Please be sure to check your local intranet for local variations and language versions of this Policy.

5 POLICY CONTROLS AND OBJECTIVES

This Policy is supported by the following control objectives, standards, and guidelines.

5.1 PRINCIPLES REGARDING USE OF ELECTRONIC RESOURCES

A. Authorized Access.
Only authorized users must have access to Electronic Resources.

B. Compliance with Laws and Policies.
When using Electronic Resources, you must always comply with any applicable laws and regulations, this Policy and the supporting policies set forth in Section 8. This includes, without limitation, protecting Personal Data in compliance with applicable data protection and/or information security laws, and the Personal Data Protection Policy.

C. Sensible Use.
Your use of Electronic Resources must be sensible and in such a manner that it does not interfere with the smooth and efficient running of the business. The Company reserves the right to alter this Policy at any time if this trust is abused.

D. Information Protection.
You must protect all information (including Restricted, Highly Confidential and Confidential information, as defined in the Company's Information Classification Policy and the Information Security Policy) owned by the Company and its licensees (for example, proprietary code) while such information is in the Company's custody.

E. Business/Personal Use.
The Electronic Resources are provided mainly for legitimate business purposes and should only be used for personal or non-business reasons on a limited basis and within reasonable limits.

Date: 10/feb/2023 Signature: Harshit

5.2 UNACCEPTABLE USES OF ELECTRONIC RESOURCES

When using Electronic Resources, you must **not** engage in any of the following:

A. Abusive, Obscene or Discriminatory Use	B. Export Controls Violations	C. Illegal or Inappropriate Activity
D. Improper Disclosure of Confidential Information	E. Legal or Other Harm to Company or Others	F. Disruption/Damage or Unauthorized Access
G. Viruses	H. Social Networks/Websites – Violation of Terms of Use	I. Advertisement or Inappropriate Solicitation
J. Impersonation	K. Sending Email Without Consent, Where Required	L. Copyright Violation
M. Install Unauthorized Software	N. Fraud/Misleading Statements or Fraudulent Email Headers	O. Unauthorized Company Warranties, Guarantees, Representations or Contractual Commitments
P. Unapproved Wired Device Connections	Q. Unsecured Wireless Connections	R. Inappropriate Sharing of Electronic Resources
S. Sending Trivial/Unnecessary Emails	T. Improper Use of Another Person's Computer or Email/ Assumed Identity	U. Unsecure Sending, Storing or Providing Access to Sensitive Personal Data

*For more details on each of the above, please see each item below.

A. Abusive, Obscene or Discriminatory Use

Using Electronic Resources in a way that is abusive, obscene, discriminatory, racist or harassing, derogatory, offensive or liable to cause embarrassment to the Company or others.

B. Export Controls Violation

Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. For example, this includes traveling outside of the United States with a laptop computer that is an Electronic Resource that contains such information.

C. Illegal or Inappropriate Activity

Engaging in any activity which is illegal under any applicable law. Such violations may constitute a criminal offense. You are prohibited from accessing websites, web-directories or similar sources hosting or containing unlawful, immoral, or criminal material, material which is liable to cause embarrassment to others, or otherwise inappropriate content (such as online gambling sites or sites containing pornographic material). The Company recognizes that it is possible to inadvertently access such sites, and you will have the opportunity to explain any accidental breaches of this Policy.

D. Improper Disclosure of Confidential Information

Disclosing or sharing Restricted, Highly Confidential and Confidential information with third parties unless such disclosure is permitted or authorized by law and a Non-Disclosure Agreement (NDA), Data Processing Agreement or other suitable agreement has been signed by authorized Company Personnel. The disclosure must also be deemed appropriate given the volume and sensitivity of the information.

Date:..10/feb/2023 Signature:.....Harshit

E. Legal or Other Harm to Company or Others

Causing legal liability for the Company or damage the Company's brand or reputation or causing damage, distress, or any other form of harm to others.

F. Disruption/Damage or Unauthorized Access

Doing anything to disrupt, damage, impair, interrupt, slow down, interfere with or affect the functionality of the Electronic Resources, including any computer hardware or software, beyond your normal use. You must not attempt to gain access to restricted areas of the Company's network, systems, databases or to any other password-protected information, unless you are specifically authorized. For the 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. You must not grant any access to the network, systems, databases or to any other password-protection information of the Company to any person who has not been duly authorized by the Company. If you are in any doubt, you must obtain written permission to the standard set out in paragraph 7 below.

G. Viruses

Knowingly uploading, transmitting or posting any material that contains viruses, worms, time-bombs, keystroke loggers, spyware, adware, Trojan Horses or any other harmful files, programs or other similar computer code designed to adversely affect the operation of any computer software or hardware.

H. Social Networks/Website- Violation of Terms of Use

Using social networks or other websites in violation of their posted terms and conditions.

I. Advertisement or Inappropriate Solicitation

Advertise or offer to sell or buy any goods and services for any business purpose, unless specifically permitted to do so by your manager. Make or circulate commercial, religious or political statements or solicitations, or promote businesses unrelated to the Company.

J. Impersonation

Impersonating another person or entity or create a false identity for the purpose of misleading another person.

K. Sending Email Without Consent or an Unsubscribe Mechanism, Where Required

Sending unsolicited email to any individual, business, or entity with whom you do not have an established business relationship or documented prior express or implied consent where such consent is required under applicable data protection law or sending email that does not have a working unsubscribe mechanism where one is required (for example, as needed to comply with CAN-SPAM, CASL, the e-Privacy Directive). If you are unsure if you need consent or an unsubscribe mechanism, please contact the Global Privacy Office.

L. Copyright Violation

Downloading, copying and/or distributing copyrighted material including, but not limited to, digitizing and distributing music, movies, games, text or photographs from magazines, books, websites or other copyrighted sources, without prior authorization by the content owner.

M. Install Unauthorized Software

Downloading or installing any software onto Electronic Resources that hasn't already received prior approval by the Company without obtaining prior authorization from the Information Security Office.

Date:10/feb/2023 Signature:Harshit

N. Fraud/Misleading Statements or Fraudulent Email Headers

Making fraudulent, misleading offers of products, items, or services. Any offers made for or on behalf of the Company must be authorized by your manager or supervisor. Engage in unauthorized use or forging of email header information.

O. Unauthorized Company Warranties/Guarantees/Representations/Contractual Commitments

Making statements about warranties or guarantees (expressly or implied) regarding the Company unless it is a part of your normal job duties and has been agreed to by your manager. Agreeing to terms, entering into contractual commitments or making representations by email unless appropriate authority has been obtained.

P. Unapproved Wired Device Connections

Connecting any device that is not a Company approved Electronic Resource (for example a personal laptop) to the Company's wired network without approval from the Information Security Office.

Q. Unsecured Wireless Connections

Conducting business activities, connecting to your email or transmitting Company information across any wireless network connection that is not properly secured according to the standards of the Information Security Office. For example, using the Company provided virtual private network (e.g., Global Connect) is considered secured and meets the standards.

R. Inappropriate Sharing of Electronic Resources

Sharing Electronic Resources with family, friends and other third parties.

S. Sending Trivial/Unnecessary Emails

Contributing to system congestion by sending, uploading, posting or forwarding unauthorized or unsolicited advertising, promotional materials, “junk mail”, “spam”, “chain letters”, “pyramid schemes” or any duplicative or unsolicited trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them.

T. Improper Use of Another Person’s Computer or Email/Assumed Identity

Sending messages from another Company Personnel’s computer or email account or under an assumed name unless specifically authorized by the Information Security Office.

U. Unsecure Sending, Storing or Providing Access to Sensitive Personal Data

Using the Company's systems to send Sensitive Personal Data via email, the Internet, instant messaging or by other means of external communication which are not known to be secure. Storing Sensitive Personal Data locally on Electronic Resources or in file shares that are not secure or providing inappropriate access to the Sensitive Personal Data.

5.3 USE OF ELECTRONIC MAIL (EMAIL) - PRECAUTIONS

A. Draft Carefully – Messages Can Be Forwarded

You should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. As emails can be easily forwarded to multiple recipients, you should assume that email messages may be read by persons other than the intended recipients.

B. Legal Production of Emails

Email messages may be disclosed in legal proceedings and provided to individuals in response to a subject access request under applicable data protection legislation, in the same way as

paper documents and other records. Even though you delete an email from your inbox or archives, that does not mean that an email cannot be recovered for the purposes of disclosure. You should treat all email messages as potentially retrievable, either from the main server or using specialized software, in accordance with Company policies and applicable laws.

C. Phishing - Emails from Unknown Sources

Phishing is the most common way for bad actors to try to compromise Company systems. You should never reply to, act on, forward, click on links or open attachments (especially any file that ends in .exe) related to emails that you believe to be a phishing attempt or when you are unsure of the source of the sender of the email. If you suspect that you have acted on such an email, you should report it immediately as an incident. If you receive an email you believe to be a phishing attempt, you should use the Company's phishing incident reporting application in Outlook or if you do not have the phishing application, then report it as an incident by following the steps outlined in Section 2.

D. Shared Email Inboxes

Shared mailboxes must be approved by the Information Security Office and have an individual assigned as the owner who is responsible for all activity involving that mailbox.

E. Receipt of Wrongly Delivered Email

If you receive a wrongly-delivered email, you must notify the sender, but you must not respond to SPAM or phishing emails.

F. Use of Email Forwarding Rules

The use of email forwarding rules set-up to forward the receipt of Company emails to non-Company email addresses is prohibited without a valid business justification which must be approved by the Information Security Office.

5.4 Use of External or Cloud Services

A. Approved External Cloud or External Hosting Services

The Information Security Office will maintain a list of approved external vendors providing cloud or external hosted Electronic Resource services to the Company, for example Salesforce.com. You may only use cloud services on the approved list. The Information Security Office will audit the approved vendors on a regular basis for compliance with the Company's security and privacy requirements and will assign each vendor a qualified level of information classification for the service.

B. Reporting Incidents Regarding Cloud Services

You must report as an incident the transmission or storage of Company information with an unapproved cloud service or the transmission or storage of Company information above the qualified level of the vendor.

5.5 Use of Electronic Resources for Payment Card (Credit Card) Transactions

If you accept payments through a payment card (any type of credit card) on behalf of the Company using Electronic Resources, you must only use Electronic Resources that have been audited and approved by the Information Security Office for compliance with the current Payment Card Industry Data Security Standard.

Date: 10/feb/2023 Signature: Harshit

5.6 USE OF THUMB DRIVES AND EXTERNAL STORAGE MEDIA

You must not transfer Company information (in any format) to external storage media or portable devices or equipment (fixed/external hard disk, USB/Memory-Stick, CDs/DVDs, etc.) not provided and, where appropriate, configured by the Company. Any such device or equipment containing Sensitive Personal Data or any other data that qualifies as Restricted under the Company's Information Classification Policy must be encrypted using a solution approved by the Information Security Office and in compliance with the Information Security Policy.

5.7 SECURITY, ACCOUNTS AND PASSWORDS FOR ELECTRONIC RESOURCES

A. Information Security Policy

You are responsible for protecting Electronic Resources as required by the Company's Information Security Policy.

B. Creating and Changing Passwords

You must create a unique password for your accounts and not re-use passwords for the same account according to the rules for that account regarding prior passwords. You must change your account password on the schedule required by the Company. You must ensure the confidentiality of your account password by not revealing it to or sharing it with others or allowing others to use your account. This includes family and other household members when work is being done at home.

C. Communicating Passwords

If you communicate passwords or other secret authentication information, you must do so securely according to the standards of the Information Security Office. For example, if you need to provide a password, do not include it in an email sent with the file that is password protected. You should instead call the receiver of the file and provide the password by phone.

D. Privileged Access Accounts

The Information Security Office will tightly control privileged access accounts (admin accounts, root accounts, etc.) and such accounts must only be created and/or issued with the approval of the Information Security Office. Privileged access accounts and their use must comply with all standards and procedures issued by the Information Security Office.

5.8 USE OF ELECTRONIC RESOURCES FOR TELECOMMUTING/REMOTE WORK

A. Working at Client Sites

As noted in the Scope section of this Policy, if you are operating at a third party site that is not controlled by the Company (for example a Company client site or remotely but for the benefit of a client) and/or using client issued Electronic Resources, in addition to the policies provided to you by the Company, you may be subject to additional policies provided to you by that third party, and you agree to comply with those policies. Unless otherwise directed by a client, you agree:

- Not to store locally on the Electronic Resources or transmit to any external device any client confidential or proprietary information or any Sensitive Personal Data, regardless of whether the Sensitive Personal Data originates from the client or some other source;
- To follow the "stand up, lock up" practice of locking the Electronic Resources when stepping away, no matter how briefly as required by the Company's Information Security Policy; and
- To not use any personal devices or personal equipment.

B. Working at Home or other Remote Worksites

Date:10/feb/2023 Signature:Harshit

If you are operating at a home office, airport, hotel or other remote site not controlled by the Company, then you are responsible for following this Policy and the Information Security Policy in those remote work environments.

C. Conflicts in Policies

In the event there is a conflict between any policies you have received from the Company and any policies you receive from a client or other third party, you should follow the Policy that best ensures the rigorous protection and safekeeping of any Electronic Resources you are using, as well as the data contained within them. If you are not sure what you should do, you must reach out to the Company and to the client or other third party for guidance.

5.9 MONITORING OF ELECTRONIC RESOURCES

For information regarding how the Company monitors your use of Electronic Resources, see the Company's Workplace Monitoring Policy.

5.10 RETURN OF ELECTRONIC RESOURCES FROM DEPARTING EMPLOYEES/CONTRACTORS

You must return all Electronic Resources that belong to the Company or to a client upon any separation of your employment or engagement with the Company (for example, laptops, mobile phones, iPads/tablets, thumb drives/storage devices, key fobs/access badges). You must return the Electronic Resources in the same condition as when it was delivered to you, absent any normal wear and tear. Upon your separation, the Company will disconnect you from all Electronic Resources, including, without limitation access to the Company's email and the Company's networks, intranet, applications (for example, Salesforce.com) or other Company-paid subscription services (for example, LinkedIn Premium or research tools) and network and file shares (for example Microsoft Team's sites and network file shares such as O:, Q:, S:, T:, and U:.

6 ENFORCEMENT

This Policy is important to the Company, and the Company intends to provide you with additional training and/or education to assist you in complying with it. In the event you violate this Policy, any one or all of the following further actions might be undertaken:

- Revoking your rights to access Company systems, physical facilities (including buildings, rooms, and file drawers), Electronic Resources, such as electronic sites (for example websites, intranet sites, team sites, SharePoint sites, social media sites), files or file shares, databases, applications, Company- provided subscription-based services or any other Company access points on a temporary or a permanent basis;
- Initiating disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning; and/or
- Initiating civil or criminal proceedings to pursue any remedies available.

7 EXCEPTION HANDLING

While every exception to a Policy or standard potentially weakens protection mechanisms for Company systems and underlying data, occasionally exceptions may be appropriate. Requests for exceptions to this Policy should be submitted to the Company Information Security Department.

Date:10/feb/2023 Signature:Harshit

Exceptions shall be permitted only on receipt of documented approval from the Company Information Security Department.

8 SUPPORTING DOCUMENTS

- Information Classification Policy
- Information Security Policy
- Personal Data Protection Policy
- Social Media Policy
- Workplace Monitoring Policy

9 DOCUMENT INFORMATION

Document Name	Acceptable Use of Electronic Resources Policy
Issue Date	January 1, 2023
Next Review Date	January 1, 2024
Author(s)	Maureen Dry-Wasson
Maintainer	Craig White
Owner	Andy Sheppard

10 VERSION HISTORY

ISSUE	DATE	DESCRIPTION OF CHANGE AND REASON
1.0	Nov. 1, 2011	First version under name “Electronic Resources Policy”
2.0	Nov. 1, 2012	Annual review
3.0	Jan. 1, 2013	Annual Review; changed to 1/1 review cycle
4.0	Jan. 1, 2014	Annual Review
5.0	Jan. 1, 2015	Annual Review
6.0	June 1, 2016	Name of Policy changed to “Acceptable Use Policy”
7.0	Jan. 1, 2017	Annual Review – updated definition of Electronic Resources and Sensitive Personal Data; added training and education to enforcement section; minor typos and wording changes
8.0	Nov. 18, 2018	Annual review – no changes made
9.0	Jan. 1, 2020	used new template; changed name of Policy to “Acceptable Use of Electronic Resources Policy; updated Policy for GDPR; revised organization to make it easier to digest for reader
10.0	Jan 1, 2021	Annual review – added examples for clarity; minor wording changes and typos
11.0	Jan 1, 2022	Annual review – added e-mail forwarding rules; updated definition of Sensitive Personal Data to match change made in other policies; minor wording changes and typos
12.0	Jan 1, 2023	Annual Review – updated definitions for Social Media and Sensitive Personal Data to match changes made to those definitions in the Social Media Policy and Personal Data Protection Policy, respectively; minor typos and wording changes

Date:10/feb/2023 Signature:Harshit

CONTROLLED SUBSTANCE TEST RELEASE AND AUTHORIZATION

TEKsystems Global Services Pvt. Ltd (The “Company”, “TEKsystems”) maintains a drug-free work environment and may require you to submit to and pass a controlled substance test as a condition of employment and as a condition of continued employment potentially for this assignment with TEKsystems, Are you willing to submit to a controlled substance test under these guidelines?

☑ **Yes** ☐ **No**

I, Harshit Mishra, have received and read a copy of The Company’s Drug and AlcoholPolicy. I have read this policy and have had the opportunity to ask questions. I agree to follow thepolicy and to accept the penalties, including among others, the penalty of immediate discharge for violating the policy. I understand that my compliance with this policy is a condition of my employment and continued employment. I hereby certify that I am not a current user of illegal drugs.

I hereby give my consent to and authorize The Company, and the testing laboratory designated by The Company, to perform the appropriate tests and procedures to identify the presence of controlled substances. I also give my permission for the results of the controlled substance test to be released to The Company and to The Company’s clients requesting my services.

I understand that refusal to take a controlled substance test, provide a sufficient amount of specimen, attempts to adulterate the sample, or a positive test result for controlled substances will result in The Company denying my application for employment or immediately terminating my employment.

I hereby release and hold harmless The Company, its employees, agents, contractors, clients and any persons or other parties disclosing information from any and all liability whatsoever arising from this request for a controlled substance test, from the testing of the sample, and from decisions made concerning my application for or continuation of employment based upon the results of the controlled substance test. I hereby authorize that a photocopy of this authorization may be construed and used as an original. I also give my permission to The Company to release the results of the controlled substance test, in defense of any claim(s) brought forth in connection with the denial of my application for employment or the termination of my employment.

I acknowledge that The Company’s Drug and Alcohol Policy is subject to change at any time without notice, and nothing contained herein shall alter or limit The Company’s right to terminate my employment at any time, for any reason, without prior notice.

Date: 10/feb/2023 **Signature:** Harshit

TEKsystems Drug and Alcohol Use Policy and Procedure

Policy Statement

TEKsystems is committed to providing a safe work environment and to promoting and protecting the health, safety and well-being of its employees, customers and clients. This commitment is jeopardized when an employee engages in the use, possession, sale, conveyance, distribution, or manufacture of illegal drugs, intoxicants, or controlled substances or abuses prescription drugs or alcohol. Substance abuse is a serious health problem and has a detrimental effect on TEKsystems, its customers and clients in terms of productivity, absenteeism, accidents, medical costs, theft and worker's compensation costs. In addition, TEKsystems will vigorously comply with applicable country law. This policy covers all employees (Full-Time Regular, Part-Time Regular, Temporary Employees (or) Consultants) Therefore, TEKsystems has established the following policy:

Policy

While on TEKsystems, client or customer premises and while conducting business-related activities of TEKsystems, client or customer premises, no employee may use, possess, distribute, sell, convey, manufacture, or have a system (blood, sweat, hair, urine or saliva) presence of any illegal drugs. The legal use of prescribed drugs is permitted on the job only if it does not impair an employee's ability to perform the essential functions of the job effectively and safely. TEKsystems will follow the applicable country law, regulation or labor agreement, or individual employment agreement, then the relevant country law, regulation or labor agreement, or individual employment agreement will supersede that section or provision and the remainder of this Policy will remain in effect.

Alcohol must not be consumed in a TEKsystems office or at a client or customer facility. Employees may not report to work, or return from lunch or other break periods under the influence of alcohol (defined as when the result of drinking any amount of alcohol impairs mental or physical faculties in such a way as to reduce the ability to act with ordinary care).

Stipulations

Violations of this policy may lead to disciplinary action, up to and including immediate termination of employment. Such violations may also have other legal consequences.

Drug and Alcohol Testing

– Who is subject to policy

Any individual on the following teams:

- Practices/Centers
- Delivery
- A project with client requirement

Date: 10/feb/2023 **Signature:** Harshit

When will Testing be Conducted?

Where permitted by law, TEKsystems reserves the right to require drug and alcohol tests of employees in the following situations:

- Post-offer; or
- Pre-employment; or
- Reasonable cause or suspicion; or
- Random; or
- Following an on the job accident which results in personal injury or property damage; or
- For other legal reasons, pursuant to the policies of the client or customer

Timeframes

- Employees must comply with instructions to submit to reasonable cause/suspicion or random substance testing immediately upon instruction
- Employees must comply with instructions to submit to post-accident testing as soon as any necessary medical treatment is completed.
- Other reasons for testing may have specific designated timeframes that the employee must comply with

Penalties

An employee's failure to immediately comply with a substance testing request within the timeframes required may lead to disciplinary action, up to and including immediate termination of employment.

Refusals to Test

Failure to appear for the test within the required timeframe, failure to remain at the testing site until the test process is complete, failure to provide the required specimen, failure to provide sufficient volume of specimen, failing to comply with re-testing following a cancelled test, or providing a specimen that has been adulterated will be treated as a refusal to test and the employee will be ineligible for hire if the test is conducted post-offer pre-employment, or if occurring for an existing employee then in that case the employee will be subject to disciplinary action up to and including termination.

The testing process starts once the collector engages the employee to start the testing process. In the event that the employee is unable to provide a sufficient volume of specimen, shy bladder/lung procedures will be followed.

Random Testing

Employees may be subject to random drug and/or alcohol testing pursuant to the policies of a customer. An employee failing to submit to the required drug and/or alcohol testing will be subject to termination.

Date: 10/feb/2023 **Signature:** Harshit

TGS IT POLICY

The following sections set out requirements that are particularly significant and provide relevant information about some of the legislation that governs the use of IT facilities. Everyone who use TGS IT facilities must comply with the policy, legislation and principles that are referred to here as well as to other directives issued by the TGS Information Technology Department.

1. ACCEPTABLE POLICY

1.1 Acceptable Use of IT facilities

Employees must not use IT facilities for the purpose of personal profit making or for commercial activities other than those of the TGS. Use of TGS IT facilities including email and the internet is conditional upon compliance with all TGS policies procedures and guidelines.

1.2 Copyright Law

Copyright law restricts the copying of software and other material subject to copyright (documents, music, broadcasts, videos etc) except with the express permission of the copyright owner.

1.2.1 Software

Employees may not make use of, or copy, software contrary to the provisions of any agreement entered into by the TGS. The onus is on employees to consult with IT department to clarify the permitted terms of use if they wish to use any software for purposes other than those for which the TGS has a license.

1.2.2 Multiple users

Copies of software used in a multi-access or network environment to allow simultaneous access by more than one user can only be provided if specifically permitted in the contract or software licence, or if a copy of the software has been purchased for every simultaneous user.

1.2.3 Email and Copyright

The copyright of an email message is owned by the sender, or the sender's employer. Copyright owners have a variety of rights, including the right to reproduce their work and the right of communication to the public. Forwarding something to an email discussion list would be construed as "to the public". Consider the expectations of the originator; did that person set any conditions on the further communication of their email, or expect that it would not be forwarded to anyone else, or would not be forwarded to a particular recipient?

1.2.4 Spam

All email messages sent from a TGS email account must comply with the Spam Act. This Act sets up a scheme for regulating commercial e-mail and other types of commercial electronic messages. The Spam Act refers to spam as "unsolicited commercial electronic messaging". "Electronic messaging" includes emails, instant messaging, SMS and other mobile phone messaging. A single message may be spam. The message does not need to be sent in bulk, or received in bulk.

Signature: ……Harshit……

1.3 Security

The following practices should be observed to maintain the security of the TGS's IT facilities.

- Employees must keep their user name and password safe and not make their password available to others or use any account set up for another user or make any attempt to find out the password of a facility or an account for which they do not have authorized access.
- Employees must ensure that the confidentiality and privacy of data is maintained
- Employees who have been granted access to computer systems are responsible for the safe keeping of the data they access.
- Employees must not divulge any confidential information that they may have access to in the normal course of their employment.
- Employees must not seek access to data that is not required as part of their duties as a Employees member of the TGS.
- Employees who inadvertently obtain data to which they are not entitled or who become aware of a breach of security pertaining to data from any information technology facility must immediately report this to the *itcompliance@TGS-inc.com* or local IT personnel. Unauthorized release or use of data inadvertently obtained may lead to legal action.
- Employees must ensure the security of their workstation by logging off or observing other security measures when it is left unattended.
- Employees shall not bring their friends/Relatives to TGS to access TGS network/internet.
- Employees shall not bring any external storage devices (HDD, USB Sticks, CD, DVD etc.) and their personal Laptops.
- Employees shall not carry out any objectionable, frivolous or illegal activity on the internet that shall damage the company's business or its image

1.4 Non - Interference

1.4.1 Inconvenience and damage

Employees must not behave in a manner which, in the opinion of relevant TGS managers and supervisors, unduly inconveniences other people or which causes or is likely to cause damage to TGS IT facilities.

1.4.2 Installation of software

Employees must not install software on any TGS IT facility unless the installation is designated as part of their authorized work.

2. UNACCEPTABLE OR PROHIBITED USE OF IT FACILITIES

2.1 Purpose

IT facilities are provided for use in the TGS's business activities. They are not provided for private personal use, although it is recognized that, as with the telephone, there will be limited use for personal purpose.

Some types of unacceptable use, for example transmission of material of an obscene nature, are specifically prohibited by the local law.

Signature: Harshit ……..

2.2 Examples of unacceptable use

Unacceptable use of IT facilities include:

- circumventing system security provisions or usage quotas
- visiting inappropriate internet sites concerned with pornography and down loading materials that are pornographic or storing or transmitting any such material
- playing computer games or other leisure activities such as joining in chat rooms or surfing the internet in pursuit of personal interests that are not related to work.
- sending or soliciting obscene, profane or offensive material.
- sending email messages or jokes that contain discriminating or sexually harassing material, or messages that create an intimidating or hostile work environment for others.
- using TGS IT facilities in the conduct of personal businesses or for commercial purposes that are not directly related to TGS business.
- using TGS email facilities to send chain letters.
- unauthorized forwarding of confidential TGS messages to persons inside and outside the TGS who are not intended to receive that message.
- using another person's mailbox without authorization.
- sending unsolicited personal opinions on social, political, religious or other non-TGS related matters, where sending such opinions is not a legitimate part of education or research.
- soliciting to buy or sell goods or services.
- using, copying or transmitting copyrighted information in a way that infringes the owner's copyright.
- Access to sites related to sports, finance, news and HR (jobs)
- Freeware / shareware / unlicensed software or tools without prior consent from authorized Personnel

2.3 Inadvertent unacceptable use

In relation to use of the web, it may not always be possible to tell if a web page is relevant until it has been read and web search engines and links can sometimes lead to irrelevant and inappropriate websites. In these cases usage logs may be used to demonstrate that access to inappropriate sites was inadvertent.

2.4 Seeking advice on use

Where Employees have doubt concerning their authorization to use any IT facility or about whether a particular use is acceptable, they should seek the advice of their supervisor or the IT Help Desk.

2.5 Use for personal purposes

There may be some use of TGS IT facilities for personal purposes that are unrelated to work (eg. internet banking). Such use must be limited, reasonable and appropriate and it must not:

- contravene TGS policy
- interfere with official use of IT facilities or
- interfere with a Employees member's obligations to the TGS.

Signature: Harshit ……..

The amount of personal use is at the discretion of a Employees member's supervisor or manager and therefore, seek advice from them before using the internet for personal purposes.

2.8 Penalties for misuse of IT facilities

Employee's members who do not abide by TGS policy when using IT facilities, may have their access to IT facilities suspended and disciplinary action, and/or legal action may be taken.

3. PRIVACY

A member of Employees may expect some privacy in relation to their use of the computer and email and internet resources the TGS makes available to them at work. Despite the use of individual passwords, privacy is limited in the following ways:

- Use of computers, email and the internet can be accessed by IT administrators
- IT systems automatically log the internet sites visited, the downloads made and the time spent at each site as well as information about emails sent and received. This automatically logged information can be accessed by IT administrators.
- while contents of emails and web sites are not routinely recorded, contents may be stored on Employees computers or on servers
- it is possible to retrieve deleted records from backups and archives.

4. MONITORING OF USE OF IT FACILITIES

4.1 Routine monitoring

The TGS provides IT facilities for use by Employees in relation to the TGS's teaching and learning, research, administrative and business activities. Routine monitoring of the use of IT facilities is conducted to monitor the costs and acceptable use of TGS resources. The type of information automatically collected includes:

Internet	Email
• the name of the person who accessed the internet site • the date and time the site was accessed • the site address (or "URL") • the computer the person used to access the internet • the size of the site or web page accessed or the amount of material downloaded.	• the email address of the person who sent the message. • the name of the person who received the message. • the email addresses of other people who received the message. • the date and time at which the message was sent and received. • the server(s) from which the message was sent.

The TGS routinely monitors the level of usage to control costs. Cost centers contribute towards these costs and cost centre managers receive summary information that allows them to monitor usage by Employees in their cost centre. The costs associated with individual use of IT resources, specifically an individual's use of the internet, are recorded.

Signature: Harshit ……..

4.2 Other monitoring

In normal circumstances, Employees supporting IT services will not monitor the contents of electronic mail messages or other communications or files they access as a result of their work (e.g. auditing operations). However, whenever the Management decides it is appropriate, the TGS will inspect, copy, store and disclose the contents of email to prevent or correct improper use, satisfy a legal obligation, or to ensure proper operation of IT facilities.

5. EMAIL BULLETINS AND DISTRIBUTION LISTS

5.1 General notices

General notice bulletins to public groups, news groups, or specific work groups can only be sent for the purposes of TGS business associated with work and by the authorized personnel.

5.3 Distribution list management

Global Distribution Lists may be created with the approval of Management. The owners of these lists are responsible for their accuracy.

6. OTHER INFORMATION

To help Employees use IT resources responsibly, the following information is provided.

6.1 Mailbox space management

- To maintain the performance and reliability of the TGS's email environment, size limits will be placed on the storage capacity for the on-line mailboxes for each user.
- All Employees can reduce their Exchange server demands by monitoring their storage usage, deleting unwanted mail or archiving email to other storage media. Employees will liaise with their local IT support Employees to ensure that local conventions for archive storage are followed and appropriate backup procedures are undertaken.
- When Employees reach 80% of their allocated quota they should work IT team to resolve.
- Employees will receive system generated messages delivered to their mailbox informing them when they have near the allocated quotas. This message does not mean that Employees will be restricted from sending email but serves as a regular reminder.
- Employees are prevented from sending and receiving any more messages when they have reached 100% of their allocated quotas. Employees have the option of removing and archiving items, or purchasing more mailbox quota space.
- Default and allocated quotas will be reviewed to ensure that 'normal' functions of Employees can be performed within the quotas allocated.
- Additional storage space for individual users may be allotted by formal approvals from reporting managers.

6.2 Procedures relating to email when an Employee leaves

- When an Employees leaves the email account is to be deleted/forward to the reporting manager to make sure nothing important is missed.

Signature: Harshit ……..

6.3 Use of public folders

- Public Folders should be used as part of workflow processes or sharing of email messages, however, they should not be used for archiving personal email data.

6.4 Use of email signatures

Employees should include a signature on all emails (sample mailed regularly). Do not include drawings, pictures, maps, and graphics in your signature or an inspirational or other type of quotation at the end. Such material is unnecessary in a business communication and may not be well-received.

I agree and accept the above terms

Employee Name: Harshit Mishra

Employee Number:

Designation: Technical Trainee

Date: 10/feb/2023

Signature: Harshit ……..