

Junior System Administrator

Roles and Responsibility

17th April, 2023

Document Version & History

Version	Author	Date	Comments
1.0			

Title	Junior System Administrator
Document ID	
Description	
Version	v1.0
Author	Envigo Technologies
Classification	
Review Date	
Reviewed by	
Approved date	
Approved By	
Release Date	
Copy Owner	
Privacy	



Scope

As a system administrator, the main responsibility is to ensure that the computer systems, networks, and servers run smoothly and efficiently


Junior System Administrator

Delivery

1. **Monitoring system performance:** During the delivery process, you may be responsible for monitoring the performance of systems and applications to ensure that they run smoothly and efficiently. This includes identifying and troubleshooting any issues that may arise.
2. **Security and compliance:** As a system administrator, you may also ensure that the systems and applications used during the delivery process are secure and compliant with relevant regulations and industry standards. This may include implementing access controls, performing security assessments, and ensuring that data is properly protected.
3. **Backup and recovery:** In case of a system or application failure, you may perform backups and manage recovery processes. This includes ensuring backup data is stored securely and accessible when needed.
4. **Documentation and reporting:** You may be responsible for documenting and reporting on the systems and applications used during the delivery process. This includes maintaining documentation on system configurations, performance metrics, security assessments, and other relevant information.

Process & Security

1. **Documentation and updating process documentation:** You may be responsible for documenting IT processes and procedures, ensuring they are up-to-date and accurate. This may include maintaining process maps, standard operating procedures (SOPs), and



other documentation that outlines how IT systems and applications should be configured and managed.


2. **Monitoring and troubleshooting:** You may also be responsible for monitoring IT systems and applications for errors or issues and troubleshooting problems as they arise. This may involve monitoring tools to track performance metrics and identify potential problems.
3. **Task automation:** As a junior system administrator, you may automate routine tasks such as backups, software updates, and configuration changes.
4. **Access control:** You may be involved in managing user accounts and access control measures. This may include setting up user accounts, configuring permissions, and implementing multi-factor authentication.
5. **Vulnerability scanning:** As a junior system administrator, you may be responsible for conducting regular vulnerability scans to identify potential security issues. This involves using vulnerability scanning tools to identify IT system and application vulnerabilities.
6. **Security awareness training:** You may be responsible for conducting security awareness training for employees to help them understand how to protect IT systems and data from security threats. This may involve creating training materials and conducting training sessions.

Onboarding:

1. **User account setup:** You may be responsible for setting up user accounts for new employees, ensuring they have the appropriate access levels and permissions.
2. **Device setup:** You may also be responsible for setting up new devices for employees, such as laptops or desktop computers. This may involve installing software, configuring network settings, and ensuring the device is secure and up-to-date.
3. **Security awareness training:** You may be involved in conducting security awareness training for new employees to ensure that they understand how to protect IT systems and data from security threats.

Offboarding:

1. **Account deactivation:** You may be responsible for deactivating user accounts and revoking access for employees leaving the organisation. This helps to ensure that former employees cannot access IT systems and data after they have left.

- 
2. Data backup and transfer: You may also be responsible for backing up and transferring data from the departing employee's devices and accounts to a secure location or a replacement employee's performance.
 3. Device recovery: If the departing employee has company-issued devices, you may be responsible for recovering them and ensuring that they are securely wiped or re-allocated to another employee.
 4. Contribute to Employee Engagement Activities and setup

Learning & Development

1. Should be capable of learning new technologies and adaptable.
2. Expand your skill and knowledge to different technologies.

Competency Required

Iceberg Elements	Competency Attributes List (Weightage)
Skills (Proficiency)	<ol style="list-style-type: none"> 1. Effective Communication (4) <ul style="list-style-type: none"> ○ Good persuasive verbal communication and written skills in English ○ Ability to form a good rapport with managers, and colleagues as part of trust-building. 2. Listening Skills (5) 3. Problem Solving Skill (4) <ol style="list-style-type: none"> a. Expecting a good problem-solving skill 4. Time Management (4) <ol style="list-style-type: none"> a. Time estimation and accuracy will be an important factor b. Finish your assignments on-time and be ready for agreed time c. Delegate parallel executions wisely based on requirement if need. d. Take necessary actions without wasting time. e. Ability to prioritize and manage time 5. Leadership (4) <ol style="list-style-type: none"> a. Do what is right, even if it is tough b. Data Driven Decision Making that is fair and communicated precisely as to why the decision was made to everyone

Knowledge (Proficiency)	<ol style="list-style-type: none"> 1. Technical Knowledge (5) <ol style="list-style-type: none"> a. Knowledge in Networking/Firewall/Access Point b. OS : Install/troubleshoot Windows,Linux ,Mac OS c. Hardware troubleshooting (Laptop/Desktop/Printer] d. Monitoring : Firewall/Access Points/Google workspace /o365/Zoho e. Security [Office N/w ,OS Security Best Practices] 2. Documentation and asset handling (4) 3. Risk Management (4) <ol style="list-style-type: none"> a. Identifying risk and finding ways for mitigating risk.
Self-Image (Perspective)	<ol style="list-style-type: none"> 1. Confident and Passionate 2. Empathetic and a people person
Traits (Perspective)	<ol style="list-style-type: none"> 1. Positive Attitude and continue to see good side of the team. 2. Accept Failures and Take Lessons 3. Empathic 4. Willingness to learn and adapt 5. Honest 6. Servant Leader 7. Approachable and Friendly
Motives (Perspective)	<ol style="list-style-type: none"> 1. Thrive for constant improvement. 2. Finds satisfaction in taking up challenges and executing them 3. Passionate about growth 4. Finds joy in impacting the lives of people and organizations positively.

PERFORMANCE MANAGEMENT GOALS

Goals are categorised into three sections

Category	Details	Weightage
Business Outcome	Goals Defined below in detail.	70%
Proficiency	Showcase growth in Knowledge and skills. This will be done in Skills-Base Tool. You would do a self-assessment, and for the given role, we will have a desired level of competency against each skill and knowledge.	10%
Perspective	Your Attitude and Traits are assessed by 360 Degree Feedback. We'll take a cross-section of your direct team, manager, peers and dotted-lined employees to get feedback. This would be part of the appraisal life cycle.	20%

Goals – Business Outcome

Category	Weightage 100	Weightage 70	Details
Delivery	35%	24%	Individual Detailed KPIs would be derived from the role sheet
Process & Security	35%	25%	
Learning & Development	10%	7%	
Team Management	10%	7%	
Process Adherence	10%	7%	

—

■ ■ ■