

P2018 - Job Monitoring Policy

Contents

Purpose:.....	3
Scope:.....	3
Statement:.....	3
Policy Sections:.....	5
Policy Compliance	5
.....	6
Policy References:.....	7
Related Procedure References:.....	7
Related Regulatory Information:.....	7

Purpose:

The Job Scheduling Policy of Integrity Marketing Group (Integrity) aims to establish a structured framework for scheduling and managing various tasks and jobs. This policy is designed to optimize resource utilization, ensure timely execution of critical processes, and enhance overall operational efficiency.

Scope:

This policy encompasses the scheduling and management of jobs across various departments within Integrity. It applies to both automated and manually scheduled tasks, covering routine operational processes, data processing, and other job-related activities.

Statement:

Roles & Responsibilities

Integrity Security Governance Committee: The Integrity Security Governance Committee is responsible for the development, implementation, maintenance, and enforcement of this policy. The Security Governance Committee must approve all data classifications proposed by data owners, work in cooperation with compliance and legal counsel to generate data retention timelines and ensure data retention efforts comply with this policy by conducting regular audits or assessments.

Integrity IT: Integrity IT Team is responsible for saving and backing up data in accordance with data retention requirements and assigning data ownership to individuals responsible for each data type. They are also responsible for the implementation of any processes and controls required to protect the organization's data.

System administrator: System Administrator shall be responsible for planning, coordinating, and overseeing the scheduling of tasks and jobs. They shall ensure that jobs are scheduled efficiently, considering resource availability and business priorities.

Stakeholder Involvement: Engage key stakeholders, including department heads, IT personnel, and process owners, in the job scheduling process. Their involvement is crucial for understanding departmental priorities and resource constraints.

Communication Channels: Establish clear communication channels between the Job Scheduling Team and departmental representatives. Regular meetings, status updates, and collaboration tools shall be utilized to facilitate effective communication.

Policy Statement

Background jobs in information systems are automated processes that execute tasks without direct human intervention. These jobs are typically scheduled to run at specific times or triggered by certain events. They're vital for system integrity, data confidentiality, and continuous operations.

Job Identification and Prioritization

Jobs must be characterized by well-defined parameters, including a unique job name, a concise description of the task, and a detailed specification of resource requirements. System Administrators must submit jobs through a designated interface, providing essential details such as a unique job name, description of the task, and a specification of resource requirements.

Each submitted job shall be assigned a priority level based on predefined criteria, considering factors such as the job's criticality, urgency, and impact on overall system performance. High-priority jobs shall be given precedence in the scheduling queue to ensure timely execution, while lower-priority tasks are scheduled accordingly.

Scheduling and Resource Allocation

A systematic scheduling process shall be established to consider the availability of resources, including personnel, technology, and facilities. Upon job submission, careful consideration shall be given to technology dependencies, and allocations shall be made based on the specified needs. To prevent resource bottlenecks and ensure efficiency, ongoing monitoring of resource usage shall be conducted, with adjustments made as necessary.

In the event of conflicting resource requests, jobs with higher priority shall be granted precedence to minimize the impact on critical tasks. Additionally, System Administrators shall be allowed to specify the importance of their jobs and request adjustments when necessary. Escalation paths and decision-making authorities shall be defined to ensure swift resolution of issues.

Job Execution and Monitoring

The system shall provide real-time visibility into job execution, resource usage, and system health. Automated alerts and notifications are configured to promptly identify and address any anomalies, failures, or delays. Additionally, regular oversight by system administrators ensures proactive intervention when necessary.

User Notification

Real time alerts for critical events shall be implemented. The job scheduling system shall be configured to trigger notifications based on specific events such as job start status, completion, and failures. Notifications shall be sent through various channels, such as email, SMS, instant messaging, or integration with centralized logging systems and shall be sent to system administrators.

Security

Only authorized users shall have the appropriate level of access to view, manage job schedules and alert configurations. Users must be authenticated before accessing job monitoring functionalities. This typically involves username and password authentication. In more secure environments, multi-factor authentication (MFA) shall be implemented for an additional layer of security.

Comprehensive audit trails and logs shall be maintained to record user activities, system events, and security-related incidents. It can be used to regularly review and analyze logs to detect and respond to potential security threats.

Job Completion and Documentation

Upon job execution, a robust completion verification process shall be initiated. The system shall perform thorough checks to ensure that each job has been successfully executed, meeting all specified criteria, and adhering to dependencies. Systems shall generate comprehensive logs capturing key information throughout the job completion process. These logs shall include details such as resource usage, execution timelines, and any encountered errors or exceptions.

Key job scheduling personnel shall also maintain detailed documentation of scheduled jobs, covering job specifications, execution details, outcomes, and troubleshooting steps. Each job shall have a clear purpose description, including the business process it supports, the data it processes or generates, and any dependencies. Personnel shall also specify the schedule and timing, along with any parameters, configuration settings, and prerequisites needed for successful execution. Describe the expected outcomes and success criteria, noting where the job's output can be found. Include a troubleshooting guide for common issues with error messages, potential causes, and recommended actions, as well as contact information for support or escalation.

Exception Handling and Issue Resolution

In the event of errors, failures, or deviations from expected outcomes during job execution, an exception handling mechanism shall be implemented for timely resolution. This entails promptly identifying the root cause of the issue, implementing corrective actions, and mitigating any potential impacts on business operations. As part of this process, it's essential to automate the generation of tickets wherever technologically feasible in a designated ticketing tool whenever a job failure occurs. There shall be an escalation process for handling issues or exceptions. Roles and responsibilities shall be defined for escalating problems to higher levels of management or specialized teams for resolution. Immediate notifications for job failures must be enabled.

Change Management Integration

Any changes to scheduled jobs shall follow the change management process. In the event of a failure that requires routine procedures (such as rerunning a job) for resolution, no formal approval shall be required. However, it shall be imperative to maintain clear and comprehensive documentation outlining the execution of the resolution process. (Please refer to the Change Management Policy)

Job Retention and Archiving

Integrity shall define the duration for retaining scheduling information and outline procedures for archiving historical data. Different types of job-related data and logs shall have defined retention periods in alignment with the organization's retention policy. When determining these retention periods, consideration shall be given to regulatory requirements, business needs, and the relevance of the data.

An archiving process shall be implemented to store historical job scheduling data effectively. This process ensures compliance with data retention policies and serves as a reference for future analysis or audits. Clear criteria shall be defined to determine when data shall be moved from active storage to archival storage, ensuring efficient management and access while meeting retention requirements.

Policy Sections:

Policy Compliance

Section Name: Policy Compliance

Statement:

Compliance Measurement

The Integrity Security Governance Committee will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Integrity Security Governance Committee in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A contractor found to have violated this policy may be subject to an immediate termination of the right to access Integrity's systems and may also include the termination of Integrity's engagement with the contractor's employer.

Policy References:

Related Procedure References:

Related Regulatory Information:

P2018 - Job Monitoring Policy

Document Author	Name: Title: Email:	Jeremy Hart Asureti - Manager jeremy.hart@asureti.com
Document Owner	Name: Title: Email: Approved Date:	Matthew Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 10/21/2025
Legal Management Approval	Name: Title: Email: Approved Date:	Duncan McQueen Assistant General Counsel duncan.mcqueen@integrity.com 1/16/2026
Executive Management Approval	Name: Title: Email: Approved Date:	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 1/21/2026

Last Published Date: 1/21/2026

Document Version Number 2.0