INCIDENT AND SERVICE MANAGEMENT INFORMATION TECHNOLOGY POLICY

Policy Code:	**TM6**
Version:	**2**
Approved by:	**The Board**
Approval Date:	**1/04/2024**
Decision No.:	**B.01.2024.05**

Table of Contents

1. INTRODUCTION

The Incident and Service Management Information Technology Policy provides a framework of governance and accountability across the institution to ensure that any incidents that affect the daily operations of the Da Vinci Institute are managed through an established process to ensure minimum disruptions.

Effective incident and service management requires a campus-wide approach with clear points of accountability for reporting and feedback at all levels in the institution. The principles of transparency, accountability, obligation to act and collaboration should be applied at each step of the incident management process. These steps include identification, notification, classification, investigation, action and evaluation. Open communication and documentation should occur throughout the entire process and in accordance with relevant legislation, standards and policies.

Incident and Service Management include any event which disrupts, or which could disrupt a service. This includes events which are communicated directly by users through the Service Desk Incidents can also be reported and/or logged by technical staff (if, for example, they notice something untoward with a hardware or network component). All events should therefore not be treated as incidents.

Many classes of events are not related to disruptions at all, but are indicators of normal operations or are simply informational. Although both incidents and service requests are reported to the Service Desk, the processes to resolve these requests are different. Service requests do not represent a disruption to agreed service, but are a way of meeting the Institution's and customer's needs and may be addressing an agreed target in a Service Level Agreement (SLA).

2. DEFINITIONS

Term	Definition
Error Log	Means a log of any abnormal activity on application software
Service Desk	Central point of contact for handling user queries and other issues
Service Level Agreement	A contract between the institution and the vendor of the system(s) to provide a range of support services, up to an agreed minimum standard. SLAs will usually specify precisely what the support procedures are to be, and the way in which a support call will be escalated through the vendor's support organisation to achieve resolution

Unified Communications (UC)	Refers to the integration of communication tools that assist people exchange ideas and do their jobs more effectively. Some communication tools, like IP telephony, presence technology and instant messaging, facilitate synchronous communication

3. LEGISLATIVE CONTEXT

The Incident and Service Management Policy is benchmarked against, and should be read in the context of the relevant legislation underpinning the principles against which institutional policies, processes and standard operational procedures are developed, implemented and maintained. These include:

i. Companies Act No. 71 of 2008
ii. Electronic Communications and Transactions Act 25 of 2002
iii. Promotion of Access to Information Act No. 2 of 2000.

Da Vinci Institute's policies:

iv. Change Management Information Technology
v. Disaster Recovery Information Technology
vi. Electronic Information and Communication Systems
vii. Finance
viii. Firewall
ix. Information Security
x. Language
xi. Privacy and Confidentiality
xii. Records and Administration Management
xiii. Reputational Risk
xiv. Wireless Communications.

4. SCOPE

This policy applies to all Da Vinci employees and other persons who have access and use Da Vinci's systems to create, access or use Da Vinci's information, and forms part of Da Vinci's Information Technology Systems, including but not limited to:

4.1. Employees
4.2. Elected Members
4.3. Contractors
4.4. Temporary staff

4.5. Partner organisations

4.6. Customers

4.7. Volunteers

4.8. Any other party utilising Da Vinci Institutes' ICT resources.

5. PURPOSE

The primary goal of the Incident and Service Management policy is to outline the processes to restore normal service operations as quickly as possible, and minimise the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.

6. VALUE TO BUSINESS

The value of Incident and Service Management includes the ability to:

6.1 Detect and resolve incidents which results in lower downtime to the business, which in turn should result in higher availability of the service enabling the business to exploit the functionality of the service as designed.

6.2 Align Information Technology (IT) activities to real-time business priorities as incident management includes the capability to identify business priorities and dynamically allocate resources as necessary.

6.3 Identify potential improvements to services. This happens as a result of understanding what constitutes an incident and also from being in contact with the activities of business operational staff.

6.4 Identify additional service or training requirements as identified by the service desk during its handling of information technology incidents. Incident and service management is highly visible to the business by demonstrating its value in the area of service operation thereby providing a justification for expenditure on implementing processes to maintain a high standard of service.

7. PRINCIPLES

Basic issues and matters that need to be taken into account and decided upon when considering incident and service management issues include the following:

20.1 Timescales must be agreed for all incident-handling stages. These will differ depending upon the priority level of the incident, and upon the overall incident response and resolution targets within SLAs.

8. INCIDENT MANAGEMENT PROCESS

8.1 An incident remains an incident forever – it may grow in impact or priority to become a major incident, but an incident never becomes a problem. A problem is the underlying cause of one or more incidents and remains a separate entity.

8.2 The Service Desk would ensure that all activities are recorded and users are kept fully informed of progress.

9. PROCESS ACTIVITIES, METHODS AND TECHNIQUES

The process to be followed during the management of an incident includes the following steps:

9.1. Incident Identification

Work cannot begin dealing with an incident until it is known that an incident has occurred. As far as possible, all key components should be monitored so that failures or potential failures are detected early so that the incident management process can be started quickly. Ideally, incidents should be resolved before they have an impact on users.

9.2. Incident Logging

All incidents must be fully logged and date/time stamped, regardless of whether they are raised through a Service Desk telephone call or whether automatically detected via an event alert.

When Service Desk and/or support staff visit customers to deal with one incident, they may be asked to deal with further incidents 'while they are there'. It is important that when this is done, a separate Incident Record is logged for each additional incident handled – to ensure that a historical record is kept and credit is given for the work undertaken. All relevant information relating to the nature of the incident must be logged so that a full historical record is maintained – and that should the incidents have to be referred to other support group(s), IT support staff will have all relevant information at hand to assist them.

9.3. The information needed for each incident is likely to include the following detail:

i. Unique reference number.
ii. Incident categorisation (broken down into sub-categories).
iii. Incident urgency.
iv. Incident impact.
v. Incident prioritisation.
vi. Date/time recorded.

vii. Name/ID of the person and/or group recording the incident.
viii. Method of notification (telephone, automatic, e-mail, in person, etc.).
ix. Name/department/phone/location of user.
x. Call-back method (telephone, e-mail, etc.).
xi. Description of symptoms.
xii. Incident status (active, waiting, closed, etc.).
xiii. Related Configuration Items (CI).
xiv. Support group/person to which the incident is allocated.
xv. Related problem/known error.
xvi. Activities undertaken to resolve the incident.
xvii. Resolution date and time.
xviii. Closure category.
xix. Closure date and time.

9.4. Incident Categorisation

Part of the initial logging must be to allocate suitable incident categorisation coding so that the exact type of the call is recorded. This will be important later when looking at incident types/frequencies to establish trends for use in problem management, supplier management and other Information Technology Service Management (ITSM) activities. The check for Service Requests in this process does not imply that Service Requests are incidents. This is simply recognition of the fact that Service Requests are sometimes incorrectly logged as incidents (e.g. a user incorrectly enters the request as an incident from the web interface).

Lower levels of categorisation refer to the level of prioritisation that may be allocated that will not cause high-level impact on the user/s or the institution and will be given a time frame of 48 hours to resolve.

10. INCIDENT CATEGORISATION

A breakdown analysis of the incidents within each higher-level category should be used to decide the lower-level categories that will be required.

The details available at the time when an incident is logged may be incomplete, misleading or incorrect. It is therefore important that the categorisation of the incident is checked, and updated if necessary, at call closure time.

11. INCIDENT PRIORITISATION

Every incident logged should be agreed upon and an appropriate prioritisation code allocated as this will determine how the incident is handled both by support tools and support staff.

Prioritisation can normally be determined by taking into account both the urgency of the incident (how quickly the business needs a resolution), and the level of impact it is causing.

An indication of impact is often (but not always) the number of users being affected. In some cases, and very importantly, the loss of service to a single user can have a major business impact – it all depends upon who is trying to do what – so numbers alone is not enough to evaluate overall priority.

11.2 Other factors that can also contribute to impact levels

i. Risk to life or limb.

ii. The number of services affected (multiple services).

iii. The level of financial losses.

iv. Effect on business reputation.

v. Regulatory or legislative breaches.

An effective way of calculating these elements and deriving an overall priority level for each incident should be determined. In all cases, clear guidance with practical examples should be provided for all support staff to enable them to determine the correct urgency and impact levels, so the correct priority is allocated. Such guidance should be produced during service level negotiations.

There will be occasions when, because of particular business expediency or other reasons, normal priority levels have to be overridden. When a user is adamant that an incident's priority level should exceed normal guidelines, the Service Desk should comply with such a request.

An incident's priority may be dynamic if circumstances change, or if an incident is not resolved within SLA target times, then the priority must be altered to reflect the new situation.

Some tools may have constraints that make it difficult to automatically calculate performance against SLA targets if a priority is changed during the lifetime of an incident. If circumstances do change, the change in priority should be made, and if necessary, manual adjustments made to reporting tools.

11.3 Initial Diagnosis

Should the incident be routed via the Service Desk, the Service Desk analyst must carry out initial diagnosis, typically while the user is still on the telephone to endeavour to discover the full symptoms of the incident and to determine exactly what has gone wrong and how to correct it.

Should the Service Desk analyst not be able to resolve the incident while the user is still on the telephone, but there is a prospect that the Service Desk may be able to do so within the agreed time limit without assistance from other support groups, the analyst should inform the user of their intentions, give the user the incident reference number and attempt to find a resolution.

12. INCIDENT ESCALATION

The exact levels and timescales for both functional and hierarchic escalation need to be agreed, taking into account SLA targets, and embedded within support tools which can be used to monitor and control the process flow within agreed timescales. The Service Desk should keep the user informed of any relevant escalation that takes place and ensure the Incident Record is updated accordingly to keep a full history of actions.

Incident ownership remains with the Service Desk at all times regardless of where an incident is referred to during its life times. The Service Desk remains responsible for tracking progress, keeping users informed and ultimately for Incident Closure.

12.1 Functional escalation

As soon as it becomes clear that the Service Desk is unable to resolve the incident itself, or when target times for first-point resolution have been exceeded, whichever comes first, the incident must be escalated immediately for further support. If the organisation has a second-level support group and the Service Desk is of the opinion that the incident can be resolved by that group, it should refer the incident to Service Operation which refers to the fulfilment of user requests via an e-mail or phone call to inform that the incident pertaining to a ticket number or reference number has been addressed and resolved, and the incident is closed, having resolving service failures, fixing problems, or performing any routine operational task.

12.2 Simple priority coding system

Impact – High, Medium, Low

i. Critical/high 1 2
ii. Urgency/Medium 3 4.
iii. Low 5.

12.3 Priority code Description Target resolution time

i. Critical 1 hour.
ii. High eight (8) hours.
iii. Medium 24 hours.
iv. Low 48 hours.

Planning is the first step in Information Technology Service Management (ITSM), referring to the planning stage and the people involved in the planning.

Should it become obvious that the incident will need deeper technical knowledge, or when the second-level group has not been able to resolve the incident within agreed target times (whichever comes first), the incident must be immediately escalated to the appropriate third-level support group. Third level support groups may be internal, and could also be third parties such as software suppliers or hardware manufacturers or maintainers.

12.4 Hierarchic escalation

Should incidents be of a serious nature, for example Priority 1 incidents, the appropriate IT manager must be notified, for informational purposes at least.

Hierarchic escalation is also used if the 'Investigation and Diagnosis' and 'Resolution and Recovery' steps are taking too long or proving too difficult. Hierarchic escalation is also used when there is contention about to whom the incident is allocated to.

Hierarchic escalation should continue up the management chain so that senior managers are aware and can be prepared and take any necessary action, such as allocating additional resources or involving suppliers/maintainers. Hierarchic escalation can be initiated by the affected users or customer management as they see fit; it is therefore important that the IT manager is made aware so that they can anticipate and prepare for any such escalation.

13. INCIDENT ALLOCATION

There may be many incidents in a queue with the same priority level; it will be the task of the Service Desk and/or Incident Management staff initially, in conjunction with managers of the various support groups to which incidents are escalated, to decide the order in which incidents should be prioritised and actively worked on. These managers must ensure that incidents are dealt with in true priority order.

14. INCIDENT INVESTIGATION AND DIAGNOSIS

In the case of incidents where the user is just seeking information, the Service Desk should be able to provide this fairly quickly and resolve the service request. Should a fault being reported, this is an incident and likely to require some degree of investigation and diagnosis.

Each of the support groups involved with the incident handling will investigate and diagnose what has gone wrong, and all such activities (including details of any actions taken to try to resolve or re-create the incident) should be fully documented in the incident record so that a complete historical record of all activities is maintained at all times.

14.1 Incident investigation actions include:

- Establishing exactly what went wrong or is being sought by the user.
- Understanding the chronological order of events.
- Confirming the full impact of the incident, including the number and range of users affected.
- Identifying any events that could have triggered the incident (e.g. a recent change or some user action).

15. RESOLUTION AND RECOVERY

When a potential resolution has been identified, this should be applied and tested. The specific actions to be undertaken and the people who will be involved in taking the recovery actions may vary, depending upon the nature of the fault.

15.1 People and actions involved in resolution and recovery:

i. Asking the user to undertake directed activities on their own desktop or remote equipment.

ii. The Service Desk implementing the resolution either centrally (example rebooting a server), or remotely using software to take control of the user's desktop to diagnose and implement a resolution.

iii. Specialist support groups being asked to implement specific recovery actions (example Network Support reconfiguring a router).

iv. A third-party supplier or maintainer being asked to resolve the fault.

Should a resolution have been found, sufficient testing must be performed to ensure that recovery action is complete and that the service has been fully restored to the user(s).

In some cases it may be necessary for two or more groups to take separate, though coordinated recovery actions for an overall resolution to be implemented. In such cases Incident Management must coordinate the activities and liaise with all parties involved.

Regardless of the actions taken, or who does them, the Incident Record must be updated accordingly with all relevant information and details so that a full history is maintained. The resolving group should revert the incident to the Service Desk for closure action.

16. INCIDENT CLOSURE

The Service Desk should check that the incident is fully resolved and that the users are satisfied and willing to agree the incident can be closed.

16.1 The Service Desk should check the following:

i. **Closure categorisation.** Check and confirm that the initial incident categorisation was correct or, where the categorisation subsequently turned out to be incorrect, update the record so that a correct closure categorisation is recorded for the incident, seeking advice or guidance from the resolving group(s) as necessary.

ii. **User satisfaction survey.** Administer a user satisfaction call-back or e-mail survey for the agreed percentage of incidents.

iii. **Incident documentation.** Pursue any outstanding details and ensure that the Incident Record is fully documented so that a full historic record at a sufficient level of detail is complete.

iv. **Ongoing or recurring problem.** Determine whether it is likely that the incident could recur and decide whether any preventive action is necessary to avoid this.

v. **Formal closure.** Formally close the Incident Record.

An automatic closure period may be chosen on specific, or all incidents, example incidents will be automatically closed after two working days if no further contact is made by the user.

Where this approach is to be considered, it must first be fully discussed and agreed with the users, and widely publicised so that all users and IT staff are aware of this. It may be inappropriate to use this method for certain types of incidents, such as major incidents or those involving Very Important Persons (VIP) such as high-ranking executives, etc.

17. RE-OPENING INCIDENTS

Despite all adequate care, there will be occasions when incidents recur even though they have been formally closed. As a result of such cases, it is necessary to have predefined rules about if and when an incident can be reopened. It should be considered that if the incident recurs within one working day then it can be re-opened, but that beyond this point a new incident must be raised, but linked to the previous incident(s). The exact time threshold/rules may vary between individual campuses, but clear rules should be agreed and documented, and instructions given to all Service Desk staff so that uniformity is applied.

18. TRIGGERS, INPUT AND OUTPUT/INTER-PROCESS INTERFACES

Incidents could be triggered in many ways. The most common route is when a user rings the Service Desk or completes a web-based incident-logging screen. Technical staff may notice potential failures and raise an incident, or ask the Service Desk to do so, and may also arise at the initiation of suppliers – who may send some form of notification of a potential or actual difficulty that needs attention.

18.1 The interfaces with Incident Management include:

i. **Problem Management:** Incident Management forms part of the overall process of dealing with problems in the institution. Incidents are often caused by underlying problems which must be resolved to prevent service operation processes from recurring.

ii. **Configuration Management:** Data is provided to identify and progress incidents.

iii. **Change Management:** Where a change is required to implement a workaround or resolution, this will need to be logged as a Request for Comment (RFC) and progressed through Change Management. In turn, Incident Management is able to detect and resolve incidents that arise from failed changes.

iv. **Capacity Management:** Incident Management provides a trigger for performance monitoring where there appears to be a performance problem. Capacity Management may develop workarounds for incidents.

v. **Availability Management:** Use Incident Management data to determine the availability of IT services anddetermine at which point of the the incident lifecycle it could be improved.

vi. **Service Level Management (SLM):** The ability to resolve incidents in a specified time is a key part of delivering an agreed level of service. Incident Management enables SLM to define measurable responses to service disruptions. It also provides reports that enable SLM to review SLAs objectively and regularly.

19. SERVICE LEVEL MANAGEMENT

Acceptable levels of service as defined within which Incident Management operates, include the following:

i. Incident response times.

ii. Impact definitions.

iii. Target fix times.

iv. Service definitions, which are mapped to users.

v. Rules for requesting services.

vi. Expectations for providing feedback to users.

20. INFORMATION MANAGEMENT

20.1 Most information used in Incident Management comes from the sources which contain information about:

i. Incident and problem history.

ii. Incident categories.

iii. Action taken to resolve incidents.

iv. Diagnostic scripts which can assist first-line analysts to resolve the incident, or at least gather information that will assist second- or third-line analysts to resolve it faster.

20.2 Incident Records, which include the following data:

i. Unique reference number.

ii. Incident classification.

iii. Date and time of recording and any subsequent activities.

iv. Name and identity of the person recording and updating the Incident Record.

v. Name/organisation/contact details of affected user(s).

vi. Description of the incident symptoms.

vii. Details of any actions taken to try to diagnose, resolve or re-create the incident.

viii. Incident category, impact, urgency and priority.

ix. Relationship with other incidents, problems, changes or known errors.

x. Closure details, including time, category, action taken and identity of person closing the record.

21. METRICS

21.1 The metrics that should be monitored and reported upon to judge the efficiency and effectiveness of the Incident Management process, and its operation, include the following:

i. Total numbers of Incidents (as a control measure).

ii. Breakdown of incidents at each stage (e.g. logged, work in progress, closed, etc.).

iii. Size of current incident status.

iv. Number and percentage of major incidents.

v. Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code.

vi. Percentage of incidents handled within agreed response time (incident response-time targets may be specified in SLAs, for example, by impact and urgency codes).

vii. Average cost per incident.

viii. Number of incidents reopened and as a percentage of the total.

ix. Number and percentage of incidents incorrectly assigned.

x. Number and percentage of incidents incorrectly categorised.

xi. Percentage of incidents closed by the Service Desk without reference to other levels of support (often referred to as 'first point of contact').

xii. Number and percentage of the incidents processed per Service Desk agent.

xiii. Number and percentage of incidents resolved remotely, without the need for a visit.

xiv. Number of incidents handled by each Incident Model.

xv. Breakdown of incidents by time of day, to assist pinpoint peaks and ensure matching of resources.

Reports should be produced under the authority of the Incident Manager, who should draft a schedule and distribution list, in collaboration with the Service Desk and support groups handling incidents.

22. CHALLENGES, CRITICAL SUCCESS FACTORS AND RISKS

22.1 Challenges

The following challenges exist to ensure successful Incident Management:

i. The ability to detect incidents as early as possible. This will require education of the users reporting incidents

ii. All staff (technical teams as well as users) to acknowledge that all incidents must be logged.

iii. Availability of information about problems and known errors. This will enable Incident Management staff to learn from previous incidents and also to track the status of resolutions.

22.2 Critical Success Factors

The following factors will be critical for successful incident management:

i. A fully operational Service Desk is key to successful Incident Management.

ii. Clearly defined targets to work to – as defined in SLAs.

iii. Adequate customer-oriented and technically training support staff with the correct skill levels, at all stages of the process.

iv. Integrated support tools to drive and control the process.

22.3 Risks

The risks to successful Incident Management are similar to some of the challenges and the reverse of some of the Critical Success Factors.

Risks include**:**

i. Being inundated with incidents that cannot be handled within acceptable timescales due to a lack of available or properly trained resources

ii. Lack of adequate and/or timely information sources due to inadequate tools or lack of integration

iii. Mismatches in objectives or actions.

23 REVIEW OF THIS POLICY

Regular review and amendment of this policy will be done in line with the approved institutional policies. This will take place in consultation with the relevant quality assurance structures at departmental and institutional level, under the auspices of the official custodian of this policy, namely the Head Information and Communication Technology.

24 REVISION HISTORY

Version No.	Amendment Details	Approval date	Approving Committee	Chairperson Signature
Version 1 (V1)	Various	01/04/2019	EXCO	
Version 2 (V2)	Amendments as per review tracking document:	11/04/2024	The Board	