Incident Management Policy of IT Security

Approval
Date: **03/11/2021**
ASI Manager: **Dr Francesca Pruneti**
Digitally signed pursuant to Legislative Decree No. 82/2005

About the document		
Edited by: *O.U. IT Security*	**Target audience:** *Users of the University of Parma*	**Filing of the document:** *www.unipr.it/regolamento-security-EN*

Summary

1. Purpose of the document

The purpose of this document is to define the proper management of IT security incidents. A good management of IT incidents is useful to protect the personal data of which the University is the owner, to guarantee the security of information and of the systems used process it, as well as to minimise the impact on the services provided and users' operations. In particular, the document indicates guidelines for IT security incidents:

- are detected and analysed in a timely manner;
- are properly managed;
- have a minimal impact;
- the necessary containment actions are taken to prevent further damage;
- incidents and the corresponding mitigation actions are recorded and documented;
- the competent authorities or interested parties are informed in a timely manner as required by current regulations.

2. Scope of application

The policy described in this document applies to the University's IT perimeter. This perimeter has changing contours which, over time, tend to take on increasingly less circumscribed characteristics and dimensions. The Athenaeum's IT perimeter consists of: IT systems, services, processes and procedures using software and hardware, but also users with different practices and habits. All the components of this IT perimeter, from the most physical to the intangible ones, may suffer or generate an IT incident, or at least be affected by it in part.

3. What are IT security incidents

An IT security incident is an event that tends to or may compromise the principles of integrity, confidentiality and availability of information managed by the University using IT tools. An event that does not have these characteristics, although it may create inconvenience to users or economic damage to the University, should not be considered an IT security incident. An event is also classified as an IT security incident if it prevents the fulfilment of legal obligations or exposes the organisation to the risk of incurring penalties or having to pay compensation for any damage caused. Below is a non-exhaustive list of events that constitute an IT security incident:

- unauthorised access to databases, computer systems, company networks or related equipment;
- unauthorised access to the perimeter of the organisation where restricted access computer equipment or apparatus is located;
- unauthorised dissemination or disclosure of information;
- compromising the integrity of systems or information;
- inability to access information processed by the organisation;
- malfunctioning of any kind of control, access and surveillance systems;
- physical or logical damage to resources containing information, or necessary for its processing, resulting in the loss or reduction of the integrity, confidentiality and availability of the information;
- spread of malware within IT infrastructure, etc.

4. What are Data Breaches?

A breach of personal data processed by the Athenaeum, also known as a "Data Breach", is a particular type of IT security incident that results - accidentally or unlawfully - in the destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed by the Athenaeum's data controller (as defined in EU Regulation 679/2016 - GDPR). A personal data breach may compromise the confidentiality, integrity or availability of personal data. For a precise definition of personal data, please refer to the document ***'Personal Data Classification Policy'***. By way of simplification, personal data means any information concerning an identified or identifiable natural person (data subject). An identifiable natural person is one who can be recognised, directly or indirectly, by means of data that characterise him or her, e.g. a first name and surname, an identification number, location data, an online identifier, one or more features of his or her physical, physiological, genetic, mental, economic, cultural or social identity (GDPR, Art. 4). Personal data breaches can occur in a wide number of cases, by way of example we mention:

- loss or theft of company (or non-company) IT equipment containing personal data (e.g. laptops, memory sticks, etc.);
- sending messages containing personal data to the wrong recipient;
- publication of personal data on publicly accessible computer resources (e.g.: publication on University websites of personal data).
- disclosure of confidential data to unauthorised persons;
- abusive access (e.g.: data breach caused by unauthorised access to systems);
- inability to access data due to accidental causes or external attacks, viruses, malware, etc.
- databases altered or destroyed without authorisation from the relevant owner;
- breach of physical security measures (e.g. forcing open doors or windows of security rooms or archives containing confidential information);

5. Classification IT security incidents

A classification of IT security incidents, together with proper analysis and documentation incident information, is crucial for a timely and effective response. Depending on the impact an incident has on the organisation and the users' ability to perform their duties, the following assessment is made.

Impact	Description
Low	- Does not cause significant damage to operations, productivity, administration and management - Causes negligible loss of confidence - Involves only unclassified data - The impact on information integrity is negligible or minor with little effect on the business - It entails a loss of information availability that can be tolerated up to two/three days - Causes negligible economic and commercial losses

	- Does not cause significant damage with regard to contractual obligations and compliance risks
Medium	- It may cause interruptions of internal activities within the organisation - It could degrade the effective operation in one part of the organisation - May cause limited negative publicity - It entails a loss of information availability that can be tolerated up to one day - There are economic and commercial interests of low competitive interest and low commercial value - May cause a minor or technical breach of legal or regulatory obligations
High	- It may cause interruptions in the organisation's own activities with some repercussions also in other organisations - may compromise effective operation in different parts of the organisation - It may cause limited negative publicity such as to influence relations with other organisations or relations with the public - Involves data classified as internal - Unauthorised modifications, or loss accuracy, are moderately critical. The impact is significant and beginning have serious repercussions on the business and its operations - Loss of availability can tolerated for up to one to two hours - There are economic and commercial interests of moderate competitive interest and moderate commercial value - May cause the violation of legal or regulatory obligations
Very high	- May cause violations and hinder possible investigative activity - May cause serious disruptions of the organisation's own activities with substantial repercussions also in other organisations - It may prevent effective operation of the organisation - May widespread negative publicity that may affect relations with other organisations, the public or other countries - Involves data classified as Confidential - Unauthorised changes, or loss of accuracy, are critical to business processes and applications - Assets must be fully available normal working hours - Economic and commercial interests of high competitive interest, commercial value - Causing high financial losses - It constitutes a serious breach of contractual obligations relating to the security information provided by third parties - May cause a serious breach of legal or regulatory obligations
Critic	- May cause exceptionally serious violations - Can cause exceptionally serious damage to the effectiveness of operational or logistical activities - Can cause exceptionally serious disruptions of the organisation's own activities with serious repercussions also in other organisations - Can seriously impede the effective operation of the organisation, possibly leading to its closure - May widespread negative publicity that may negatively affect relations with other organisations, the public or other countries - Involves data classified as confidential

	- Unauthorised changes or loss of accuracy are very critical. The impact is very serious and the consequences may lead to the total failure of some or all business processes/applications. - The assets involved must ALWAYS be available - There are economic and commercial interests of the highest competitive value - Cause of exceptionally high financial losses - It constitutes an exceptionally serious breach of contractual obligations relating to security of information provided by third parties - May cause an exceptionally serious breach legal or regulatory obligations

6. IT Security Event Management

Incidents are handled through a sequence of distinct phases:

- accident preparation
- detection, identification and analysis;
- containment, eradication and recovery;
- post-accident activities.

6.1. Pre-accident activity

Incident response methodologies emphasise the proactive and continuous use of tools, training and processes necessary to prevent incidents by ensuring that systems, networks and applications are sufficiently secure. Preparedness includes all activities to respond to an incident: policies, tools, procedures, effective action plans and communication, and implies that affected groups have established the necessary controls to recover and continue operations after an incident is discovered. Post-mortem analyses of previous incidents must form the basis for continuous improvement.

6.2. Detection, identification and analysis

The first steps in detecting, verifying, investigating and analysing an incident are important for the development of an effective containment and eradication strategy. Once an incident is confirmed, resources can be allocated to investigate the necessary scope, impact and response. The detection and analysis phases determine the source of the incident and preserve evidence; this information must be communicated to the

IT Security O.U. that maintains and updates 'University IT Security Incident Register'.

6.3. Containment, eradication and recovery

Containment is the triage phase in which the compromised system or service is identified, isolated or otherwise mitigated and when affected parties are alerted. Containment procedures attempt to actively limit the scope and scale of the attack. Containment involves the acquisition, storage, securing and documentation of all evidence. Containment must prevent data from leaving the network through affected machines and prevent the attacker from causing further damage to company resources.

Eradication is the removal of malicious code, or inappropriate profile or access. Eradication also includes dealing with vulnerabilities that may have been the root cause of the compromise.

6.4. Post-accident activities

All incident response activities will be documented and reviewed post-mortem to assess whether the investigation process was effective. Subsequent corrections can be made to the methods and procedures used to improve the incident response process.

Documentation provides an opportunity to improve incident response processes and identify recurring problems. This phase also allows the analysis of the incident for its procedural implications, the collection of metrics and the incorporation of best practices into future response and training activities.

Document Revisions

Ver.	**Description of changes**	**Author**	**Date modification**
1.0	*Initial version*	*O.U. IT Security*	*21/05/2021*