CitNOW

CitNOW IT & Data Security Policy

Last Updated:
24th July 2018

www.citnow.com

English Version

CitNOW Business System(s): All Reference: ISO/IEC 27001 and 27002

Index

Appendix

1. Information security policy

1.1 Overview

Information is a key resource in our organisation. Information stored by us includes: customer names, email addresses, mobile number, vehicle registration number; customer eVHC information; administrative, personnel and financial data; computing network and database systems; computer code and scripts. In whatever form information is collected, accessed or used, we will ensure it is protected by appropriate security measures, enabling us to meet our business goals, conform with applicable laws and meet our contractual obligations.

1.2 Purpose

Our security objective is to protect our organisation from security problems such as: unauthorised access to systems, breaches of confidentiality (people obtaining or disclosing information inappropriately), integrity (information being altered or erroneously validated, whether deliberate or accidental) and availability (information not being available when it is required) or any other matter which may adversely affect our business operations or the business operations of our customers and suppliers.

1.3 Scope

This policy covers all computers, servers and software operated by us.

1.4 Policy

1.4.1 Approach

We will:

Use all reasonable, appropriate, practical and effective security measures to protect our processes and assets in order to achieve our security objective.

Utilise an ISMS according to ISO/IEC 27001 as a framework for guiding our approach to managing security.

Continually review our use of security measures so that we can improve the way in which we protect our business.

Protect and manage our information assets to enable us to meet our contractual, legislative and privacy responsibilities.

1.4.2 Responsibilities

All employees, past and present, permanent and temporary of ours will, at all times, act in a responsible, professional and security-aware way, maintaining an awareness of and conformance to this Policy.

All employees will respect the information assets of third parties whether or not such protection is required contractually or legally.

All employees who have supervisory responsibility are required to actively promote best practice amongst their supervised staff.

Our CISO reporting directly to our CEO, is responsible for ensuring that information within our organisation is adequately protected and for ensuring that our security objective is achieved. The CISO and the Security Panel are authorised by the CEO to pursue appropriate activities and actions that contribute to achieving our security objective and that are consistent with this Information Security Policy.

1.4.3 Practices

We will identify our security risks and their relative priorities, responding to them promptly and implementing safeguards that are appropriate, effective and practical.

All information (including third party information and personal information) will be protected by security controls and handling procedures appropriate to its sensitivity and criticality.

Where authorised to do so, information will be made available outside of our organisation to third parties. Information owners will be responsible for identifying to whom their information may be released and shall keep full and accurate records of such disclosure.

We will ensure that our activities can continue with minimal disruption, or other adverse impact, should it suffer any form of disruption or security incident.

Actual or suspected security incidents will be reported promptly to the Security Panel, who will manage the incident, and arrange for an analysis of the incident and consequent lessons to be learnt. Security incidents which relate to personal data shall be managed in compliance with applicable Privacy Law.

Documented procedures and standards, along with education and training, will support this Policy.

Compliance with the Policy will be monitored on a regular basis by the Security Panel that will meet on a regular basis.

Our CISO will facilitate an annual review of this Policy by the Security Panel. It will be reviewed for completeness, effectiveness and usability. Effectiveness will be measured by our ability to avoid security incidents and minimise resulting impacts.

Our CISO will approve all new versions of the Information Security Policy. All employees of ours are responsible for identifying ways in which the Information Security Policy might be improved. Suggestions for improvement should be sent to the Security Panel. If immediate changes are required a special meeting of the Security Panel will be called, otherwise suggestions will be discussed at the meeting to conduct the annual review of the Policy.

1.4.4 Policy Awareness

A copy of this Policy will be made available to all employees currently employed, or when they join our organisation. Individual sections of the Policy will be updated as required and will be available on our Podio Intranet site. All our employees are expected to be familiar with, and to comply with, the Information Security Policy at all times. The members of the Security Panel will, in the first instance, be responsible for interpretation and clarification of the Information Security Policy. Employees requiring further information on any aspects of this Policy should discuss their needs with a member of the Security Panel.

1.4.5 Applicability and Enforcement

This Policy applies to all of our employees and those who use its facilities and information. Compliance with the Policy will form part of the contract of employment and all employees will be responsible for their actions relating to information security.

Failure to comply with the Information Security Policy could harm our ability to achieve our aims and security objectives and could damage the professional reputation of the organisation. Failure to comply will, in the ultimate sanction, be treated as a disciplinary matter. Our CISO will be responsible for all decisions regarding the enforcement of this policy, utilising the disciplinary procedures at his or her disposal as appropriate.

We will encourage the adoption and use of this Information Security Policy by third parties cooperating in joint ventures.

2. Server security policy

2.1 Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2.2 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by our organisation. Effective implementation of this policy will minimise unauthorised access to our proprietary information and technology.

2.3 Scope

All employees, contractors, consultants, temporary and other workers at our organisation and our subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by us or registered under internal network domain owned by us.

2.4 Policy

2.4.1 General Requirements

All servers deployed at our organisation must be owned by an operational group that is responsible for system administration. Any servers dealing with customer data must be owned by the DevOps group. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the Security Panel. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the Security Panel. The following items must be met:

- All servers must be registered with DevOps. At a minimum, the following information is required to positively identify the point of contact:
- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable
- Information given to DevOps must be kept up-to-date
- Configuration changes for production servers must follow the appropriate change management procedures

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

2.4.2 Configuration Requirements

Operating System configuration should be in accordance with approved Security Panel guidelines.

Services and applications that will not be used must be disabled where practical.

Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

Servers should be physically located in an access-controlled environment.

Servers are specifically prohibited from operating within our office premises.

2.4.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online on the server for a minimum of 1 week.
- Logs should then be configured to transfer to the global log server for archive and storage.

Security-related events will be reported to the Security Panel, who will review logs and incidents. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorised access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host

2.5 Policy Compliance

2.5.1 Compliance Measurement

The Security Panel will verify compliance to 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.

2.5.2 Exceptions

Any exception to the policy must be approved by the Security Panel in advance.

2.5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3. IT asset control and disposal policy

3.1 Overview

All employees and personnel that have access to organisational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organisational assets. The asset control policy will not only enable organisational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organisational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking policy will enable the organisation to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for an asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

3.2 Purpose & Responsibility

This policy is designed to protect the organisational resources on the network by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organisational assets and will reduce risk of losing data due to poor planning.

The CTO is ultimately responsible for the development, implementation and enforcement of this policy.

3.3 Assets Tracked

This section defines what IT assets should be tracked and to what extent they should be tracked.

3.4 IT Assets Types

This section categorises the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Mobile phones and tablets
4. Printers, Copiers, FAX machines, multifunction machines
5. Handheld devices
6. Scanners
7. Servers
8. Firewalls
9. Routers
10. Switches
11. Memory devices

3.4.1 Assets Tracked

Assets which cost less than £100 shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

1. Hard Drives
2. Temporary storage drives
3. Tapes with data stored on them including system backup data
4. Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes

3.4.2 Small Memory Devices

Small memory storage assets will not be tracked by location but by trustee. These assets include:

1. Floppy disks
2. CD ROM disks
3. Memory sticks

If these types of devices are permitted for some employees, the trustee of the device must sign for receipt of these devices in their possession. All employees must also agree to handle memory sticks, floppy disks, and CD ROM disks in a responsible manner and follow these guidelines:

1. Never place sensitive data on them without authorisation. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
2. Never place customer date on them.
3. Never use these devices to bring executable programs from outside the network without authorisation and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network should be discussed with the IT department beforehand for authorisation.

See the Removable Media Policy for further information.

3.5 Asset Tracking Requirements

All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.

An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.

When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database

3.6 Transfer Procedure

3.6.1 Asset Transfer Checklist

When an asset type listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Checklist must be filled out by the trustee of the item and approved by an authorised representative of the organisation. The trustee is the person whose care the item is in. If the item is a workstation, then the trustee is the most common user of the workstation. For other equipment, the trustee is the primary person responsible for maintenance or supervision of the equipment.

The trustee must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new trustee, or being disposed of. The following information must be filled in:

1. Asset Type
2. ID number
3. Asset Name
4. Current Location
5. Designated Trustee
6. New Location
7. New Trustee
8. Locations of Sensitive Data

Once the trustee fills out and signs the Asset Transfer Checklist form an authorised representative must sign it.

3.6.2 Data entry

After the Asset Transfer Checklist is completed, it will be given to the asset tracking database manager. The asset tracking database manager will ensure that the information from the forms is entered into the asset tracking database within one week.

3.6.3 Checking the database

Managers who manage projects that affected equipment location should check periodically to see if the assets that recently were moved were added to the database. The database should provide a recent move list which can be easily checked. Managers should check the database weekly to be sure assets moved within the last 2 or 3 weeks are included in the database.

3.7 Asset Transfers

This policy applies to any asset transfers including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset trustee including when an employee leaves or is replaced.
4. Asset disposal, including:
5. Asset returned to manufacturer or reseller due to warranty return
6. Leased asset returned to Lessor

In all these cases the asset transfer checklist must be completed.

3.8 Media Sanitisation

When transferring assets to another trustee, any confidential information on the device must be protected and/or destroyed. The method of data destruction is dependent on the sensitivity of the data on the device and the next user of the device (within the organisation and its controls or outside the organisation).

3.9 Asset Disposal

Asset disposal is a special case since the asset must have any sensitive data removed during or prior to disposal. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) – No requirement to erase data but in the interest of prudence normally erase the data using any means such as sanitisation, physical destruction or degaussing.
2. Low (Sensitive) – Erase the data using any means such as electronic sanitisation, physical destruction or degaussing.
3. Medium (Confidential) – The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.

4. High (Secret) – The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved technologies are to specified in a Media Data Removal Procedure document by asset type including:

    1. Floppy disk
    2. Memory stick
    3. CD ROM disk
    4. Storage tape
    5. Hard drive
    6. RAM memory
    7. ROM memory or ROM memory devices

3.10 Media Use

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

1. Floppy disk
2. Memory disk
3. CD ROM disk
4. Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data assessment process.

1. Unclassified – Data may be removed with approval of the first level manager and the permission is perpetual for the employee duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.

2. Sensitive – Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
3. Confidential – The data may only be removed from secure areas with permission of a Vice -president or higher level of management. There must be some security precautions documented for both the transport method and at the destination
4. Secret – – The data may only be removed from secure areas with the permission of the President or higher level of management. There must be some security precautions documented for both the transport method and at the destination
5. Top secret – The data may never be removed from secure areas

3.11 Employee owned devices

This policy defines the types of employee owned devices that can be used by employees on company premises.

1. Personally owned mobile phones can be used on the premises, but should not be connected via Wi-Fi to the company network.
2. No other employee owned devices are permitted to be used on company premises, and must not be connected to the company wired or Wi-Fi network.

3.12 Enforcement

Since data security and integrity along with resource protection is critical to the operation of the organisation, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorised representative.

3.13 Employee Training and Acknowledgment of policy

Each employee in the organisation is expected to be aware of current policies and procedures related to IT Security and shall be trained on these policies and procedures on at least an annual basis. Employees are required to sign an acknowledgment that they are aware of the policy and will meet its requirements.

4. Removable media policy

4.1 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations.

4.2 Purpose

The purpose of this policy is to minimise the risk of loss or exposure of sensitive information maintained by us and to reduce the risk of acquiring malware infections on computers operated by us.

4.3 Scope

This policy covers all computers and servers operating in our organisation.

4.4 Policy

Our employees may only use removable media in their work computers which is owned by us. Our removable media may not be connected to or used in computers that are not owned or leased by us without explicit permission of Our Security Panel. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. Customer data should never be stored on removable media.

Exceptions to this policy may be requested on a case-by-case basis and can only be approved by the Security Panel.

4.5 Policy Compliance

4.5.1 Compliance Management

The Security Panel will verify compliance to 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.

4.5.2 Exceptions

Any exception to the policy must be approved by the Security Panel in advance.

4.5.3 Non–Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Virus and malicious code policy

5.1 Overview

This policy and procedure covers our Virus and Malicious Code policy.

5.2 Purpose

The purpose of this policy is to explain the approach that should be taken within our organisation to prevent against viruses and malicious code, and what to do in the event of an infection.

5.3 Scope

This policy covers all computers and servers operating in our organisation.

5.4 Policy

Given that attackers are now moving away from attacks that are merely a nuisance or destructive towards activity that is motivated by financial gain, malicious code attacks have become more sophisticated and a significant concern to organisations. A large-scale malicious code attack, often referred to as a malicious code outbreak, can cause widespread damage and disruption to an organisation, and necessitate extensive recovery time and effort. It is therefore crucial to implement adequate preventive measures, such as deploying protection and detection tools, to safeguard an organisation from malicious code attacks.

However, there is no such thing as bulletproof protection in the world of information security. It is also important that the organisation develop a robust information security incident procedure so that personnel are better prepared to handle malicious code outbreaks in a more organised, efficient and effective manner.

An incident response process should have three main stages: “Planning and Preparation”, “Response” and “Aftermath”. This section outlines the steps in the stages “Response” and “Aftermath” which are important to the complete handling of a malicious code outbreak. For more information about the “Planning and Preparation” stage, please refer to the section “Security Incident Handling for Company” policy.

The “Response” Stage consists of the following five steps:

- Detection and Identification
- Escalation
- Containment
- Eradication
- Recovery

5.4.1 Detection and Identification

5.4.1.1 Determine fully if a malicious code outbreak has occurred

The objective of this step is to determine whether a malicious code outbreak has occurred. Typical indications of a malicious code outbreak include any or all the following:

- Users complain of slow access to the Internet, exhaustion of system resources, slow disk access, or slow system boots.
- A number of alerts have been generated by a Host-based Intrusion Detection System (HIDS), or by anti-virus or malicious code detection software
- There is significantly increased network usage.
- A number of access violation entries have been noticed in perimeter router logs or firewall logs.
- A surge of out-bounced SMTP traffic originating from an internal IP addresses has been detected.

- A large number of port scans and failed connection attempts have been detected.
- The system administrator notices an unusual deviation from typical network traffic flows.
- Security controls such as anti-virus software and personal firewalls have been disabled on many hosts.
- General system instability and crashes.

Upon discovery of any of the above symptoms, IT staff should immediately check and validate all suspicious activity to determine if an outbreak has occurred. Once it is confirmed that this is a malicious code security breach, it is important to collect information about the malicious code, as this will be essential for the containment and eradication process.

Information about the malicious code can be obtained from anti-virus software vendors' websites if the malicious code has been around for some time, by reviewing alerts from anti-virus and malicious code detection software, by examining firewall and router log files. The following questions can help identify the characteristics of the malicious code:

- What kind of malicious code is it (Network worm, mass-mailing worm, virus, or trojan horse etc.)?
- How does the malicious code propagate (By attacking vulnerable network service? By mass mailing?)
- If the malicious code propagates by attacking vulnerable service, what is the vulnerability being exploited? Has a patch for addressing the vulnerability been released? What are the services or ports that are being attacked?
- Does the malicious code plant backdoors on the infected system?

- How can the malicious code be removed from the affected system? Are there any removal tools available?

5.4.1.2 Perform preliminary assessments

Once an outbreak is identified, IT staff should assess the scope, damage and impact of the outbreak in order to effectively deal with it.

5.4.1.3 Record all actions taken

IT staff should record all actions taken to deal with the outbreak and any corresponding results. This can facilitate incident identification and assessment, and provide evidence for prosecution or other useful information for subsequent incident handling stages. Logging should be carried out throughout the whole security incident response process.

5.4.1.4 Containment

The third step of response to a malicious code incident is containment. The following are activities that should be carried out in the containment stage:

5.4.1.5 Identify infected systems

Clearly identifying the infected systems is always the first step in containment. Unfortunately it is also a very complicated process due to the dynamic nature of today's IT environment. The following are some suggestions that may help identify infected systems in a managed environment:

- Perform thorough virus scanning on all the systems with the latest virus signatures as well as with updated anti-virus detection and repair engines. As no single anti-virus software or malicious code detection tool can uncover all types of malicious code, it may be necessary to use more than one anti-virus scanning tool to ensure that all malicious codes are detected
- Review all log files of routers and firewalls
- Provide users with instructions on how to identify infections
- Configure IPS or IDS to identify activities associated with infections
- Perform packet sniffing routines to look for the network traffic matching the characteristics of the malicious code

5.4.1.6 Contain the outbreak

Containing the outbreak can be done in various ways; the following are common tactics:

- By using automated tools
  Containing the spread of the malicious code can be done with automated tools, such as anti-virus software or malicious code detection tools, IDS and IPS. If the malicious code is not detected by existing anti-virus protection systems, even with the latest signature applied, support from anti-virus software vendors should be sought to create a new signature which covers the malicious code.

- By disabling connectivity
  A malicious code outbreak can be effectively contained by quickly disconnecting infected systems from the overall network infrastructure, which can be accomplished by applying access controls on network devices or physically disconnecting network cables. In some cases, in order to contain the spread of malicious code to other sections of the organisation, it may be necessary to temporarily disconnect the network segments concerned from the network backbone. However, this containment strategy will certainly affect the operation of other non-infected systems in the segment.
- By disabling services
  Malicious code may propagate through network services, for example network shared drives. Temporarily blocking or even shutting down the network services used by malicious codes helps to contain incidents.
- By eliminating vulnerability
  Malicious code may spread by attacking vulnerable network services. By addressing the vulnerabilities that have been exploited by the malicious code, such as applying security patches on vulnerable systems, the propagation channels can be eliminated, hence containing the spread. In addition, some mis-configuration, such as loose access controls on network-shared drives, can also be leveraged by malicious code. By rectifying any mis-configurations, the spread of a malicious code can be contained.

- By user participation
  User participation is significant to the containment process in an environment where only a limited number of technical support staff are available to handle an outbreak, for example in small remote branch offices or in a non-managed office environment. Users should be provided with clear instructions on how to identify infections and what measures should be taken if a system is confirmed infected, such as running the anti-virus removal tools on the infected system.

5.4.1.7 Keep records of all actions taken

It is important to keep a solid record of all actions taken at this stage, because some containment measures may require temporary modifications to the configuration or settings of network infrastructure and systems. These modifications will need to be removed after the incident.

It is important to understand that stopping further infection by the malicious code does not necessarily prevent the further damage to infected systems. For instance, the infection can be contained through disabling network connectivity. Yet, the malicious code may be still actively deleting files on the infected system. Therefore, a full eradication process should be carried out as soon as possible or in parallel with the containment process.

5.4.2 Eradication

Eradicating a malicious code outbreak should be designed to remove the malicious code from all infected systems and media, and rectify the cause of the infection. Prior to carrying out the eradication process, it is advisable to collect all necessary information, including all log files, which may have to be deleted or reset during the clean up process, which will be useful in subsequent investigations.

Anti-virus or malicious code scanning software and removal tools are commonly used as the primary means of eradication. However, in some cases, it may be necessary to rebuild infected systems from scratch. For instance, if the malicious code has downloaded and planted a backdoor on infected systems, rebuilding all systems may be the most reliable action to be taken in order to restore the integrity of the systems. Rebuilding a system generally includes the following actions:

- Reinstalling the system from a trusted source, such as system installation disk or trusted, clean system image.
- Securing newly installed systems, such as checking and ensuring that the latest virus signatures as well as the updated anti-virus detection and repair engines, and necessary security patches have been applied on each machine
- Restoring data from known, clean backup media.

5.4.3 Recovery

Clearly, the main purpose of the recovery step is to restore all systems to normal operation. In a malicious code outbreak, recovering the functionality and data of infected systems may have already been carried as part of the eradication process. Apart from restoring the infected systems, removing any temporary containment measures, such suspended network connections, is another main aspect of the recovery process.

Prior to removal of the containment measures, one important step is a pre-production security risk assessment to ensure that no infection is detected, and that the cause of the original infection is rectified.

All related parties should be notified before the resumption of suspended services. IT personnel should restore specific functions and servers stage by stage, in a controlled manner, and in the order of demand, e.g. the most essential services or those serving the majority should resume first. After resuming the suspended services, it is important to verify that the restoration operation has been successful and that all services are back to normal operation. Additional monitoring measures may be implemented to watch for any suspicious activity in the network segments concerned.

5.4.4 Aftermath

Restoring infected systems to normal operation does not mark the end of a malicious code outbreak. It is also important to perform necessary follow up action. This may include full evaluation of the damage caused, system refinements to prevent recurrence of the incident, updates to security policies and procedures, and investigation of the case for subsequent prosecution. Activities in this stage can include the following:

- Review the effectiveness of existing virus / malicious code protection procedures and mechanisms, including central control and management on virus signature distribution and detection and repair engine update, scheduled regular virus scanning, etc.
- Update relevant policies, guidelines and procedures whenever necessary.
- Enforce the new security measures introduced in the reviewed policy / guidelines / procedures to protect systems against future attacks.

- Remind users to follow security best practices, such as not opening email from unknown/suspicious email sources, updating security patches and virus definitions on a regular basis and whenever necessary, etc.

6. Incident management procedure

6.1 Purpose

The purpose of this policy is to ensure quick detection of security events and weaknesses, and quick reaction and response to security incidents.

6.2 Scope and Users

This policy is applied to the entire Information Security Management System (ISMS) scope, i.e. to all employees and other assets used within the ISMS scope, as well as to suppliers and other persons outside the organisation who come into contact with systems and information within the ISMS scope.

Users of this policy are all employees of ours, as well as all above mentioned persons.

6.3 Reference

- ISO/IEC 27001 standard, clauses A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
- ISO/IEC 27001 standard, clauses 16.1.1, 16.1.2, 16.1.7, and 18.1.2

6.4 Policy

An information security incident is a “single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security” (ISO/IEC 27000:2009).

6.4.1 Receipt and classification of incidents, weaknesses and events

Each employee, supplier or other third party who is in contact with information and/or systems of our organisation, or those of its customers, must report any system weakness, incident or event which could lead to a possible incident in the following way:

1. All information and communication technology-related events must be reported to our Security Panel, chaired by the Security Officer.
2. All other events must be reported to our Support desk

Incidents, weaknesses and events must be reported as soon as possible, by phone, email, or in person. The person who received the information must classify it in the following way:

(a) Security weakness or event – no incident occurred, but the event related to a system, process or organisation may trigger the occurrence of an incident in the near or further future

(b) Minor incident – an incident which cannot significantly impact confidentiality or integrity of information, and cannot cause long-term unavailability

(c) Major incident – an incident which can incur significant damage due to loss of confidentiality or integrity of information, or may cause an interruption in the availability of information and/or processes for an unacceptable period of time Complaints involving intellectual property rights happening in the cloud infrastructure providing services to the customer must be treated as minor incidents by the person who received the information.

6.4.2 Treatment process for security weaknesses or events

The person who received the information about a security weakness or event analyses the information, establishes the cause and, if necessary, suggests preventive and corrective action.

In situations involving online services, or the customer's PII, the Security Officer must decide if customers, to whom the security weakness or event relates, must be informed (if the customer was not the one that made the initial event report). Where customers must be informed, notifications must be made as soon as possible, by phone or in person, following agreed procedures.

6.4.3 Treating minor incidents

If a minor incident was reported, the person who received the information, in coordination with the customer's staff and when necessary or required, must take the following steps:

1. Take measures to contain the incident
2. Analyse the cause of the incident
3. Take corrective actions to eliminate the cause of the incident
4. Inform persons who were involved in the incident, as well as the Security Officer, about the incident treatment process

The person who received information about a minor incident must log the incident with the Security Officer via email, and raise a defect in Jira to alert the development team.

6.4.4 Treating major incidents

In the case of major incidents that could disrupt activities for an unacceptable period of time, one of the following procedure will be carried out:

During working hours:

1. An emergency meeting of the Security Panel is called
2. The incident is assessed for security and severity
3. A decision is made on the best course of action
4. The action is carried out
5. As soon as possible, an analysis of the cause of the incident is carried out and reviewed by the Panel

Outside of working hours:

1. The first person to be notified of the incident rounds up the technical resources they can find
2. The incident is assessed for security and severity, and whether attempting a fix out of hours could cause more damage if the right resources are not available
3. A decision is made on the best course of action
4. The minimum action is carried out
5. During working hours, a more detailed assessment is carried out with further action if necessary
6. As soon as possible, an analysis of the cause of the incident is carried out and reviewed by the Panel

6.4.5 Learning from incidents

The Security Panel must review all minor incidents every three months, and enter recurring ones, or those which may turn into major incidents on the next occasion, in the Incident Log.

The Security Panel must analyse each incident recorded in the Incident Log (identifying type, relatedness, and cost of incident) and, if necessary, suggest preventive or corrective action.

6.4.6 Disciplinary actions

The Security Officer must invoke a disciplinary process for each violation of security rules, in conjunction with the HR department.

6.4.7 Collection of evidence

The Security Panel will define the rules on how to identify, collect and preserve evidence that will be accepted as evidence in legal and other proceedings.

In situations involving the customer's PII, the Security Officer will define together with the cloud service customer the procedure to identify, collect, and preserve evidence that will be accepted as evidence in legal and other proceedings.

6.5 Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Incident Log	Company Azure	Security Panel	Only members of the panel has the right to edit the log	5 years
Rules for identifying, collecting and preserving evidences	Company Azure	Security Officer	Only the Security Officer has the right to edit and publish the rules	Records are stored for a period of 5 years

Only the Security Officer can grant other employees access to the records.

6.6 Validity and document management

This document is valid as of 24th July 2018.

The owner of this document is the Security Officer, who must check and, if necessary, update the document at least once every six months.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- Number of weaknesses or incidents which were not reported to authorised persons
- Number of incidents which were not treated in the most adequate manner
- Number of incidents which were not recorded in the Incident Log
- Number of incidents for which evidence for legal action was inadequate
- Number of violations of security rules where no disciplinary process was invoked

Previous versions of this procedure must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

7. Backup policy

7.1 Purpose

The purpose of this document is to ensure that backup copies are created at defined intervals and regularly tested.

7.2 Scope and Users

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all the information and communication technology within the scope.

Users of this document are our employees.

7.3 Reference

ISO/IEC 27001 standard, clause A.12.3.1

7.4 Policy

7.4.1 Backup Procedure

Backup copies must be created for all software systems, data and video.

Creating backups is an automated process, and is part of the software systems written and deployed by us. The head of DevOps is ultimately responsible for ensuring that backups are made and stored successfully.

Logs of the backup process are automatically created on systems where the backup copy is made.

System software is stored in a number of repositories, and uses Git, making it possible to go back to previous versions as part of the system.

Data is automatically replicated to slave databases on other servers in other data centres. Binary backups are taken hourly and stored in Amazon S3. Overnight backups are taken daily and stored in Amazon S3.

Videos are duplicated across to Amazon S3 as soon as they are processed. They remain on the primary server and S3 for a minimum of 5 days. Once deleted from the primary server, they are stored only on S3, however S3 is configured to offer high redundancy.

7.4.2 Testing backup copies

The software system repo is tested daily with developers working on it.

Data backups are tested daily as the backup is restored onto a staging server that acts as part of the deployment process.

Video backups are constantly tested as the videos are played back from the backup system after the initial 5 day period, and an anomaly script highlights any videos that have not been copied to the S3 backup.

7.4.3 Managing records kept on the basis of this policy

The software system repo is tested daily with developers working on it.

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Backup process logs – electronic form	System executing the backup procedure	Head of DevOps	Logs are read-only; they cannot be deleted or edited	Logs are stored for a period of 2 years

7.4.4 Validity and document management

This document is valid as of 24th July 2018.

The owner of this document is the CTO, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

Number of unsuccessful backup tests

Previous versions of this policy must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

Appendix

I. Security Panel Details

The security panel is comprised of at least the following roles:

- Board Director responsible for development and security (CTO)
- Chief Information Security Officer (CISO)
- Chief Software Architect
- Head of DevOps
- Head of Development

The panel must meet monthly.

The panel will review any incidents reported in the previous month, including any reports from a post mortem of the incident, and recommend changes to the system, practices, procedures or policies.

The panel will review the incidents against a list of customers, and if any are affected, will contact the customer in question using the agreed method.

II. Incident Log

Incidents are classified into the following types:

- Information related (directly related to information or communications technology)
- Non-information related (all other incidents)

Information about the incidents:

The Incident Log is a Google Document.

No.	Date of incident	Short description (name) of incident	Person responsible for handling the incident	Detailed description – impacts, duration, systems/data affected by the incident, etc.	Costs [in local currency] – direct and indirect	Reference to the Corrective Action Form
1						
2						
3						
4						