COMMISSIONER OF COMMUNICATIONS | Digital Security Authority

NCC-CY CYPRUS CYBERSECURITY COORDINATION CENTRE

ΙΔΡΥΜΑ ΕΡΕΥΝΑΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑΣ

# CYBER-HYGIENE FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES (SMEs)

**Digital Security Authority (DSA)**

**National Cybersecurity CENTRE (NCC-CY)**

**October 2023**

# CONTENTS

# TABLES



# GRAPHS

## COMMISSIONER'S MESSAGE

In the digital transformation era, in which we find ourselves in, Cyprus has deeply penetrated into digital reform aiming at the upgrading of the digital maturity of society at all levels. An upgrade that could not omit the backbone of our economy, the Small and Medium Enterprises (SMEs), which support and accelerate the growth and innovation of our economy. However, their treasure is their data. Thus, protecting a business's data ensures functionality while expanding inventiveness.

The Digital Security Authority (DSA) as the National Cybersecurity Coordination Centre (NCC-CY) works in a coordinated manner, in cooperation with the public and private sectors, research and technological bodies as well as, the academic and scientific community in order to improve the level of cybersecurity, especially for SMEs. NCC-CY encourages the implementation of the Cyber-Hygiene Framework for SMEs to enable them to effectively meet the modern challenges of the digital era.

By implementing the Cyber-Hygiene Certification, SMEs will strengthen their competitive advantage, protect their infrastructure and information, and be given the opportunity to stand out in the market. In addition, the implementation of the control measures by the Cyber-Hygiene Framework will ensure trust, integrity and availability of their information, thus increase the protection their business. Additionally, SMEs will gain confidence in the operation of their infrastructure, as they will be flexible and have a higher level of control over cybersecurity issues.

Cybersecurity is a team effort and needs everyone's contribution. NCC-CY promotes collaboration and seeks to seal the safety of every business through the Cyber-Hygiene certification. Our vision is to provide SMEs with a healthy environment to develop their potential by minimising as much as possible the risks involved.

George Michaelides

Commissioner of Communications

# CYBER-HYGIENE FRAMEWORK

# FOR SMALL AND MEDIUM ENTERPRISES (SMES)

## FOREWORD

By a decision of the Council of Ministers on 21 December 2021, the Digital Security Authority (DSA) was designated as the National Cybersecurity Coordination Centre (NCC-CY) in the Republic of Cyprus.

The NCC-CY has the mission to maintain and enhance the level of Cybersecurity in the Republic of Cyprus and to strengthen the respective efforts and contribute accordingly at the level of the European Union. One of the NCC-CY's actions is to support the community in generating innovation, but also to strengthen and develop Cybersecurity especially in Small and Medium Enterprises (SMEs), with the ultimate goal of making the Republic of Cyprus a leader in the field of Cybersecurity, ensuring at the same time a reliable and protected cyberspace for all citizens and businesses.

The NCC-CY, within its mandate, and in order to strengthen and develop Cyprus' Cyber Resilience, particularly in building cybersecurity measures for small and medium enterprises (SMEs), highlights and analyses key cybersecurity control measures as advanced best practices and tips. This document enables SMEs to assess their current level of maturity, identify their vulnerabilities and mitigate risk, while enhancing their cybersecurity practices in order to invest properly in the protection of their information and data.

# INTRODUCTION



Source: European Commission - Annual Report on European SMEs 2021/2022 (SME AR 2021_22_Final Report)

## SMALL AND MEDIUM ENTERPRISES

According to the Recommendation of the Commission of the European Communities dated 06/05/2003 and No. 2003/361/EC the definition of "Small and Medium Enterprises" (SMEs) is defined on the basis of:

- the number of employees
  *They employ <250 people*
- the turnover or the total balance sheet
  *They have ≤ €50 million annual turnover or ≤ €43 million annual total balance sheet.*

As stated on the European Commission's website:

"*Small and medium enterprises (SMEs) are the backbone of the European economy. They represent 99% of all enterprises in the EU. They employ around 100 million people, account for more than half of Europe's Gross Domestic Product and play a key role in adding value in every sector of the economy. SMEs bring innovative solutions to challenges such as climate change, resource efficiency and social cohesion and help to spread this innovation across Europe's regions. They are therefore crucial to the EU's dual transition to a sustainable and digital economy. They are essential for Europe's competitiveness and prosperity, industrial ecosystems, economic and technological dominance and resilience to external shocks.*"[1]

[1] https://single-market-economy.ec.europa.eu/smes_el?etrans=el

# SMEs IN CYPRUS

According to data issued by the Statistical Service of Cyprus and the data of CYSTAT-DB[2] , the number of enterprises in Cyprus that employ up to 249 persons, regardless of economic activity exceeds (data updated 21/12/2021) 100,000.

The distribution of potential SMEs[3] (according to the number of employees) is shown in Table 1.

| 2018 | | 2019 | | 2020 | | |
|---|---|---|---|---|---|---|
| Number of enterprises | | Number of enterprises | | Number of enterprises | | |
| 0-9 | 10-49 | 0-9 | 10-49 | 0-9 | 10-49 | 50-249 |
| 95,879 | 4,443 | 101,550 | 4,655 | 103,836 | 4,550 | 714 |

*Table 1.*

Table 1 also shows that the number of enterprises in this category is increasing every year.

# SMEs AND CYBERSECURITY

During 2021, ENISA (European Union Agency for Cybersecurity) conducted an analysis on the ability of European SMEs to cope with the cybersecurity challenges arising from the recent COVID19 pandemic[4] .

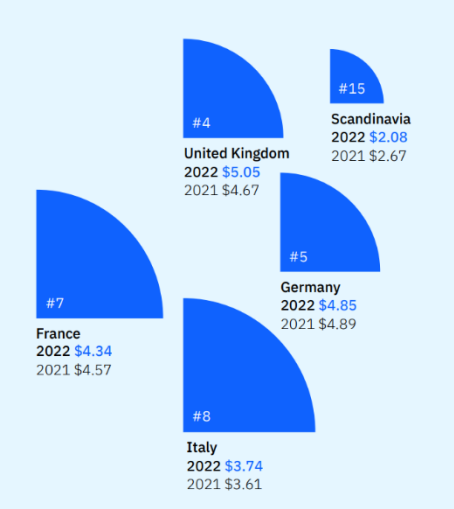
Some of the conclusions of the analysis are as follows:

- European SMEs appear to understand that cybersecurity is an important issue and that they are highly dependent on the ICT infrastructure.
- More than 80% of European SMEs surveyed, say that potential cybersecurity incidents would have a very significant negative impact on their business even in the first week after the incident occurs.
- 36% of the European SMEs surveyed responded that they had a security incident in the last 5 years.
- European SMEs seem to implement some of the key measures only as part of the overall IT implementation. However, it seems that, unless these measures are part of an IT solution, many SMEs do not comprehend the cybersecurity risks they are facing.

[2] https://cystatdb.cystat.gov.cy/ with control measures: Financial activity: TOTAL, Years 2018, 2019, 2020 and business size 0-9 persons and 10-49 persons.

[3] Possibly because there is a second control measure relating to turnover or the annual balance sheet for which no data are provided in this source.

[4] Cybersecurity for SMEs, Challenges and Recommendations, June 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes




Average cost of a data breach by country or region
Source: Cost of a Data Breach Report 2022, IBM
3R8N1DZJ (ibm.com)

**Cost of security incidents**

On the other hand, it is worth noting that "Cyber-attacks continued to increase in the second half of 2021 and 2022, not only in terms of types and numbers, but also in terms of their impact"[5], while the cost per average incident is steadily rising.

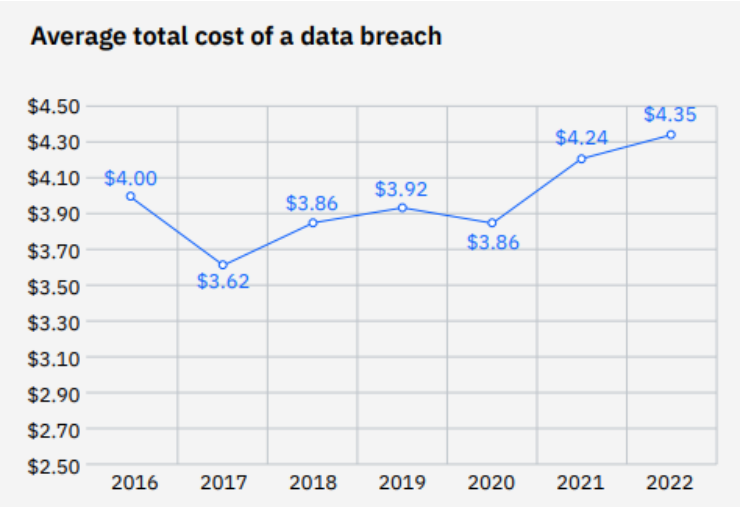
As stated in the IBM report[6] :

- The average cost of a data breach reached a high level in 2022.
- The cost per record of a data breach reached its highest level in seven years

Additionally, according to a nationwide survey conducted by the Digital Security Authority in 2022[7] , it was found that:

- Almost half of the businesses (46%) have been attacked/breached in the last 12 months, with an average of 3-4 attacks per month.

Out of the businesses that were attacked, almost half (48%) suffered financial costs of an average of €23000 each.




Calculated in US$

*Figure 1. Average cost value for each data breach[6]*

[5] ENISA Threat Landscape Report 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport
[6] Cost of a Data Breach Report 2022, IBM, https://www.ibm.com/downloads/cas/3R8N1DZJ
[7] https://dsa.cy/category/press-releases/consumers-survey

# PURPOSE OF THE PRESENT DOCUMENT

**The Digital Security Authority (DSA) as the National Cybersecurity Coordination Centre (NCC-CY) having recognized that,**

- SMEs in Cyprus represent the largest share of the economy and professional activity, and their contribution towards the stable and upward growth of the Cyprus economy is very important
- the impact of cybersecurity incidents can have adverse effects and disrupt the proper functioning and continuity of the operation of SMEs

**has decided to draw up the present document of measures aiming at:**

- the development of a cybersecurity culture in SMEs. The present document provides a comprehensive set of rules, control measures and procedures for a baseline level of cybersecurity that businesses should have in place to protect themselves from cyber threats, in order to establish or develop an adequate level of cybersecurity,
- providing guidance on cybersecurity in the form of concrete practical measures,
- increasing SMEs' awareness on issues and ways to protect themselves from cyber threats,
- motivating SMEs to promote the implementation of key cybersecurity measures through a structured approach,
- the creation of a uniform, minimum level of cybersecurity in all businesses in Cyprus,
- simplifying and adapting existing standards for information security management systems (such as ISO/IEC 27001:2022[8] , NIST SP 800-53 (revision 5)[9] , NIST SP 800-171 (revision 2)[10] and others) to the needs of SMEs.

[8] https://www.iso.org/standard/27001
[9] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[10] https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

# CONTROL MEASURES FOR CYBERSECURITY FOR SMEs

The Digital Security Authority (DSA) as the National Cyber Security Coordination Centre (NCC-CY) conducted a study to identify and analyse standards, guidelines and other publications that describe cybersecurity control measures at an international and national level. The documents reviewed concerned practices proposed for implementation by organisations, more particularly by SMEs.

The DSA, as the NCC-CY has taken into account the results of the above analysis and created this control measures document.

**The cybersecurity control measures for SMEs are divided and analysed in the following sections of the document**:


The order in which the SMEs cybersecurity control measures are presented does not indicate the order/priority of their implementation.

# 1. SECURITY POLICY

## PURPOSE

Through the cybersecurity policy, an organisation informs internal and external stakeholders of its commitment and objectives in relation to cybersecurity.

## CONTROL MEASURE 1.1

The organisation's senior management has created, approved and communicated its cybersecurity policy internally and externally. The cybersecurity policy shall be reviewed at least once a year and updated as required.

## DESCRIPTION

The cybersecurity policy is the highest hierarchical document of an organisation in relation to security. The cybersecurity policy, at a minimum, contains the following:

- A statement of the organisation's commitment to comply with cybersecurity-related legal, regulatory and contractual requirements.
- A statement of the organisation's commitment to comply with the control measures in this document and any amendments and/or guidance issued by the Digital Security Authority.
- A high-level description of the measures implemented by the organisation in relation to cybersecurity.
- A reference or summary in an appropriate annex of other policies established by the organisation that are relevant to the issue of cybersecurity.
- The designation of a senior management person to act as a point of contact between stakeholders and the organisation on cybersecurity issues.
- A statement of the organisation's commitment to responding to security incidents in a timely manner and informing stakeholders accordingly.
- A statement of the organisation's commitment to implement appropriate corrective and/or preventive actions in the event that these are officially required by authorised stakeholders (e.g. audit organisation etc.).

The cybersecurity policy will be communicated in an appropriate manner and the effectiveness of the communication will be verified, with the organisation's staff, within the framework of control measure 2.1. The cybersecurity policy is available, while maintaining the principle of ''need to know'', to external stakeholders.

Senior management has the responsibility to recognise changes in the external and/or internal environment of the organisation and to update the policy and other measures of the organisation as required.

# 2. AWARENESS AND TRAINING

## PURPOSE

The Staff is aware of cyber threat protection issues and confidently operate the relevant functions within their role.

## CONTROL MEASURE 2.1

Staff employed by the organisation and users who have access to its information (regardless of their employment relationship) must be aware of information security and in particular how they contribute to it through their role. Appropriate cybersecurity awareness activities shall be carried out on a regular basis and at least once a year.

## DESCRIPTION

Cybersecurity awareness activities aim to inform the staff of their responsibilities regarding the organisation's cybersecurity and the means by which they implement them.

Cybersecurity awareness activities should be designed taking into account the roles of the staff in the organisation, including internal and external staff (e.g. external consultants, vendor staff). Cybersecurity awareness activities should be planned at least annually, so that activities are repeating and at the same time train new employees.

Cybersecurity awareness activities can be implemented by internal or external staff, follow formal outlines and themes, or follow themes designed by the organisation itself.

## CONTROL MEASURE 2.2

Staff employed by the organisation and users who have access to its information (regardless of their employment relationship) receive education, training and information on the policies, procedures, security measures implemented by the organisation and relevant technological or organisational issues. The training provided shall be appropriate and tailored to the security requirements of the different roles within the organisation.

## DESCRIPTION

The organisation should identify and list, by job role, the key responsibilities and competencies in relation to cybersecurity.

As a minimum, all job roles will include responsibility for adhering to the policies, procedures and security measures implemented by the Organisation and related to their role.

Where additional security functions and responsibilities are recognised, minimum knowledge, skills and competencies required for their correct and effective implementation should be documented.
The organisation should identify, prepare and implement an appropriate training plan to cover knowledge gabs, skills and competencies where these 1) do not already exist and 2) require updating.

The awareness and training programme should take different forms [e.g. lectures or self-teaching, be led by qualified staff or consultants (on-the-job training), and staff members involved in different activities]. Similarly, training methods can be delivered in classroom, remotely, or through specific applications, etc.

Training and awareness activities shall be evaluated in terms of their effectiveness. Records shall be kept both with regards to the provision of the training and awareness as well as for its effectiveness.

# 3. SOFTWARE UPDATE

## PURPOSE

The organisation's IT and communication systems have fewer vulnerabilities and are therefore less exposed to the risks involved.

## CONTROL MEASURE 3.1

The organisation's IT and communications systems must have the latest security updates installed provided only from trusted sources (e.g. the manufacturer).

## DESCRIPTION

All systems have vulnerabilities, which can be exploited by a malicious factor and cause damage to the organisation.

The organisation needs to identify the information and communication systems that relate to its information and support its important activities.
It should be noted that these systems can be computers, laptops, mobile devices (e.g. tablets, mobile phones, etc.), telecommunication systems (e.g. VoIP call centres), servers, devices connected to the internet and the organisation's network (e.g. televisions or other IoT devices).

To the extent that the above systems allow automatic updates, these should be enabled. Where the option of automatic updates is not available, a manual check for updates should be implemented by qualified staff at least once a month.

Particularly for servers, security updates that are of high and medium criticality, should be installed within three months of the vulnerability detection and after testing either on another non-critical system, or after confirmation from the vendor or other parties (e.g. IT service providers) that it will not cause significant problems.

## CONTROL MEASURE 3.2

Automated vulnerability scanning and penetration tests are implemented once a year.

## DESCRIPTION

To ensure that there are no significant vulnerabilities in the organisation's IT and communications systems, automated vulnerability analysis/scanning is required at least once a year. This activity may be performed by the organisation itself or by another person provided that the appropriate equipment/software and properly trained staff are in place. The results of the vulnerability scan shall be demonstrated in a report, which shall be provided

to the organisation's management and shall include (inter alia) the vulnerabilities detected by the organisation's systems, and classification according to their level of risk. The organisation should take immediate action

to address the confirmed[11] vulnerabilities that are classified as high category (CVSS 7-10[12] ), and create a plan to manage the confirmed vulnerabilities that are classified as medium category (CVSS 4-6).

Penetration tests are carried out in order to make a meaningful and practical assessment of the security level of the organisation against relevant threats. Once a year, the organisation should conduct an external penetration test by an entity with appropriate knowledge, experience and equipment. The results of each penetration test shall be outlined in a report, which shall be provided to the organisation's management and shall include (inter alia) references to any successful access to the systems, the scenarios and steps taken during the tests (successful and unsuccessful), and recommendations on how to correct vulnerabilities. The organisation should take immediate action to address what is indicated as significant in the relevant report (points of successful penetration).

## CONTROL MEASURE 3.3

Information and communication systems that are no longer supported by their manufacturers with (at least) end-of-life security updates shall not be used by the organisation.

## DESCRIPTION

IT and communication systems that are no longer supported by their manufacturers with (at a minimum) end-of-life security updates are a major weakness for an organisation's cyber security. This is due to the fact that vulnerabilities may have arisen (in the period from end of life to the present day) which present a high risk of exploitation by malicious users, and for which there is no way of addressing or resolving them.

The organisation should monitor the dates beyond which there will be no relevant support for the information and communication systems and take appropriate preventive action to replace, change or upgrade them.

If there is an IT and communication system that is at the end of its useful life (End of Life), and which cannot be replaced or upgraded or changed (legacy), additional security measures should be taken with the agreement of the organisation's management (e.g. separation from the rest of the network, access restriction, specific operating hours, removal of rights, etc.).

[11] By confirmed vulnerabilities it is meant that a process of confirming the existence of the vulnerability in the organisation's systems has been carried out. Confirmation is important as a false positive result may occur.
[12] https://www.first.org/cvss/

# 4. PROTECTION FROM MALICIOUS SOFTWARE

## CONTROL MEASURE 4.1

Malicious software protection programmes and functions are installed throughout the organisation's IT and communication systems. Updates are made on a regular basis.

### PURPOSE

The organisation's information and communication systems are protected against malicious software's.

## DESCRIPTION

Malicious software means any software that is intentionally designed to cause disruption to an information or communications system or a set of systems (e.g. a network), leak information, gain unauthorised access to information and systems, deny a user access to information or alter stored or transmitted data. Examples of malicious software types include (among others) viruses, worms, Trojan viruses, spyware, adware, and ransomware.

Every IT and communications system (where feasible and where a solution exists) should have a malicious software protection service or feature installed or enabled. The installation/activation of the relevant protection should apply to all systems regardless of their manufacturer, operating system or type.

The automatic download and installation of programs/functions update should be enabled and the relevant check for updates (of the programs and the relevant signatures and other file updates) should be activated at least once a day.

Anti-malware programs and features should automatically scan files and programs (e.g. when downloading and opening files from the Internet, when opening files from storage media or network sources, etc.) and web pages when accessing them.

Once a week, a full scan should be performed automatically and if a threat is detected, appropriate actions should be implemented immediately.
Malicious software protection programs and features should have tamper protection enabled, so that protection cannot be disabled accidentally or maliciously.

# 5. NETWORK SECURITY

## PURPOSE

The organisation's information and communication systems are protected against threats from the public external network.

## CONTROL MEASURE 5.1

The organisation has installed and configured firewalls at appropriate points in its network, in order to effectively protect its systems and information from relevant threats.

## DESCRIPTION

The organisation should examine the network architecture it has implemented and introduce a firewall at a minimum, between the external network and the public external network (internet) and then at any other point deemed necessary to increase protection.

The firewall(s) can be either hardware or software and can be configured by adopting the positive policy (i.e.: all features, ports, protocols are denied and then only what is strictly necessary is enabled – deny all by default).
The firewall(s) will have enabled mechanisms for monitoring and logging the actions that take place, so that actions that may affect the security of information and/or systems can be detected. Logs shall be kept for at least 6 months.

The firewall(s) must have the option to protect against malicious software (e.g. viruses) enabled.

If the organisation deems it necessary, it may introduce a system for detection and/or automated penetration protection (IDS/IPS).
Remote access to authorised individuals in the organisation is only conducted through secure channels such as VPN (virtual private network). The firewall(s) should be properly configured to allow connection only after proper user-level and device-level authentication and control. Only specific and authorised devices in the organisation are allowed access to the organisation's network via VPN.

The requirements of control measure 3.1 apply as foreseen in the case of firewalls. The results of the application of control measure 3.2 shall be taken into account in its effective configuration.

The configuration data of the organisation's firewall(s) is kept in a file that is part of the backup policy as required by control measure 6.1.
Changes to the configuration of the firewall(s) are only allowed for specific, documented reasons. Changes shall only be made by authorised staff.

## CONTROL MEASURE 5.2

If the organisation provides the capability for wireless access to the organisation's network, this should be done with appropriate routing and protection through the installed firewall(s).

## DESCRIPTION

Users outside the organisation should not be able to connect to the wireless network used as an extension of (in connection with) the internal network.

If the organisation wishes, wireless access to the public external network (internet) can be provided for the visitors of the organisation in a way that is completely isolated from the rest of the internal network. This can be achieved either through a second completely separate connection to the public external network (internet) or through the firewall with appropriate configuration so that this access is completely separated from that to the internal network (only access to the public external network (internet) will be provided).

The wireless network (either internal or guest) must be protected with WPA2 encryption and above (e.g. WPA3).

Access to the management environment of the involved equipment (in the wireless network) will be strictly limited to specifically authorised and appropriate staff.

The requirements of the control measure 3.1 apply as foreseen in the case of the wireless network equipment. The results of the application of the control measure 3.2 shall be taken into account in its effective configuration.

# 6. BACKUPS

## PURPOSE

Backups of the organisation's critical information ensure its availability, integrity and confidentiality against relevant threats.

## CONTROL MEASURE 6.1

The organisation identifies its critical information and backs up its critical information on a regular basis in accordance with the relevant backup policy.

## DESCRIPTION

An organisation's information is an important asset. Certain information may be so critical to the organisation that any loss, even partial loss or total disclosure to unauthorised parties or its alteration may have significant adverse effects on the organisation.

To protect this information, organisations are required to identify their critical information (as defined above) and then take regular backups of either the information or the systems hosting it in accordance with the relevant documented backup policy.

Since each organisation has different operational requirements, different laws and regulations to which it is subject and different objectives and strategies, subsequently the timing of backup, frequency, retention period, medium and storage point are determined in accordance with the results of the relevant Business Impact Analysis – control measure 11.1.

At a minimum, the organisation should implement a 3-2-1 strategy regarding backups of critical information:

- A minimum of three (3) backups of critical information will be maintained. The first backup shall be considered the production copy (the system that the organisation uses for its day-to-day operations).
- The second backup may be located on site, provided that it is not connected to the production system. The backup should be taken at least once a day at an appropriate time so that it can be completed without causing significant problems to the operation of the organisation and the completion of the process.
- The third backup should be located in a different location from the previous two (2) and at a sufficient distance so that it cannot be easily affected by an incident occurring on the premises of the organisation. The backup should be taken at least once a week at an appropriate time so that it can be completed without causing significant problems to the operation of the organisation and the completion of the process.
- The storage medium or process should be protected from unauthorised access through the implementation of appropriate encryption. This copy may also reside in a cloud computing service that provides the desired level of protection.
-

Appropriate staff will be tasked with monitoring the proper completion of the backup download and will perform relevant recovery tests (to confirm effective operation) at least once a week.

If an organisation uses cloud computing services and does not have an extensive internal structure, then the above 3-2-1 policy is maintained with the following modifications:

- At least 3 backups of critical information will be kept. The first backup is considered to be the production backup which in this case is located in the cloud.
- The second backup may be located on appropriate storage equipment on the premises of the organisation. The backup should be taken at least once a day at an appropriate time so that it can be completed without causing significant problems to the operation of the organisation and the completion of the process.
- The third backup should be located in a different location from the previous 2 or in a different cloud provider from the production one. The backup should be downloaded at least once a week at an appropriate time so that it can be completed without causing significant problems for the organisation's operations and process completion. The storage medium or process or data should be protected from unauthorised access through the implementation of appropriate encryption.

# 7. ACCESS CONTROL

## PURPOSE

The organisation's information is organised and available only to relevant authorised parties, resulting in better management and reducing the possibility of unauthorised access.

## CONTROL MEASURE 7.1

The organisation shall identify the places where important information a is located. For the information and based on the type, the use and the criticality, the organisation has created a structure in an appropriate storage area, which allows it to grant access rights to authorised and authenticated users following the need-to-know principle.

## DESCRIPTION

The need-to-know principle implies that the user will only have access to the information they need in order to be able to perform their role effectively.

The organisation should identify for each piece of information, which role needs access to it and at what level. The organisation will maintain a list of access rights (role and level of access) by category or group of information, how access is granted (e.g. specific storage medium, applications, systems, etc.).

The levels of access identified will be at least:

- Full access: there is no restriction on the actions the user can perform on the information or the application.
- Right to change: The user can perform actions to make changes to the information, including in some cases deletion.
- Read-only access: The user can access and view the information but cannot perform any further actions.

Changes to access rights will be controlled and appropriately authorised. In the event of a change, the list of access rights mentioned above will be updated. Access to unauthenticated users should not be allowed. Authentication should be done through appropriate mechanisms that provide the desired level of security, at least through the use of a username and password combination in accordance with control measure 7.2.

User access accounts are uniquely assigned to unique individuals and account sharing is not allowed.

For special cases of systems that do not allow multiple accounts, additional measures should be introduced to allow for tracing and matching to a natural person.

In the event of retirement or a change of job, changes to access rights should be made immediately.

## CONTROL MEASURE 7.2

The organisation has created, implemented in all its systems an appropriate password policy and maintains it as well.

## DESCRIPTION

The organisation should create a password policy that contains the minimum rules regarding passwords or other means of authentication.
At least, this policy will include:

- The number of characters in the passwords. The number of characters cannot be less than 8.
- The type of characters of the passwords. As a minimum, passwords should consist of at least 3 categories (indicative categories: upper case letters, lower case letters, numbers, special characters).
- The obligation to encrypt passwords.
- The obligation to change passwords at least every 42 days. In case this is not allowed by the respective system, the other features as mentioned above should be changed (increased) accordingly to ensure an acceptable level of security.
- The obligation to keep a password history so that at least the 6 previous passwords cannot be used.

Especially for the case of remote access and access with full/administrative rights, the use of multi factor authentication is recommended.

## CONTROL MEASURE 7.3

Administrative rights or privileged rights (admin/privileged rights) are given to the minimum necessary authorised staff.

## DESCRIPTION

Individuals and roles that have administrative or privileged rights are recorded in the list of access rights referred to in control measure 7.1. The granting of such rights is strictly controlled and is only given where required to carry out the relevant tasks.

Accounts with administrative or privileged rights shall not be used in day-to-day operations that do not require such level of rights.
Installations of new software and capabilities shall be performed only by accounts with administrative or privileged rights, after appropriate staff review.

The actions of accounts (including those with administrative or privileged rights) are recorded in relevant logs and kept for at least 6 months.

# 8. SECURITY INCIDENTS

## PURPOSE

The organisation is better prepared against a security incident. The existence of appropriate forecasts allows a quick, efficient and coordinated response to security incidents.

## CONTROL MEASURE 8.1

The organisation has established a structure and process for responding to security incidents. The staff involved in the respective procedures are appropriately trained.

## DESCRIPTION

The measures implemented by an organisation cannot guarantee a total protection of data and systems. Even in cases where the organisation implements strict security measures, there will be some residual risk, a weakness or a mode of attack that has not been addressed. A security incident is one event or a series of unwanted or unexpected security events that have a significant likelihood of affecting business processes and threatening the security of the organisation's information.

As can be inferred from the above, preparing for incident response is very important for the organisation, and this is achieved by having predefined procedures (which have been tested for effectiveness) and by training staff to respond to incidents.

The organisation should establish a procedure for responding to security incidents which should include at least:

- The appointment of a person from senior management responsible for managing incidents. Such person should have or acquire appropriate knowledge to enable them to carry out the role effectively.
- The designation of the team to respond to security incidents with individual roles as required. Members of the team may include parties external to the organisation, subject to an appropriate recorded agreement.
- The definition of the systems being monitored and the ways in which information/notification of a potential security incident or event can be obtained.
- The description of the steps to be taken covering the whole life cycle of an incident (preparation, identification and recording, assessment and decision, response, completion and lessons learned).
- The definition of the ways and means by which information will be provided to stakeholders throughout the life cycle.

- The control measures for triggering the incident response mechanism.
- The method of recording, the interested parties that need to be informed or called for assistance, a relevant timeline starting at the moment of recognition that a security incident exists and the minimum information that should be included in each notification on a case-by-case basis.

Incidents involving personal data will be clearly foreseen and included in the security incident response procedure. Please note: if a data breach occurs that compromises the rights and freedoms of data subjects, the organisation must notify the Office of the Commissioner for Personal Data Protection (https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument) within 72 hours after the breach becomes known.

# 9. PHYSICAL SECURITY MEASURES

## CONTROL MEASURE 9.1

The organisation has adopted physical security measures to protect the systems and facilities from any natural and environmental threats.

## DESCRIPTION

The locations where information and communication systems equipment are installed, as well as the locations where the organisation's information (on any medium) is hosted, should be protected from physical unauthorised access and environmental conditions and disasters.

The minimum security measures that should be implemented by the organisation are:

- Locks on windows and doors.
- Alarms placed in appropriate locations and activated outside working hours (the alarm will have individual activation/deactivation codes known only to the authorised user – the assignment of passwords or access cards follows control measure 7.1.)
- Controlled access to locations that store or process critical information or house critical equipment (e.g. access control with individual passwords known only to the authorised user – the performance of passwords or access cards follows control measure 7.1).
- Fire protection, according to the relevant study (taking into account the specific conditions and the way the premises are used at the current time).
- Provision for continuous escort of visitors by the appropriate staff person.
- Power cables must be separated from mains cables to avoid interference. Mains cables shall be protected by conduits and, where possible, routes through public areas shall be avoided.
- Measurement of temperature and humidity and, where possible, automatic notification if they are out of range.
- Protection against damage, vandalism and theft depending on the location and accessibility of the site.

### PURPOSE

The organisation is more protected from threats from the physical environment, whether it is unauthorised physical access or impacts as a result of an environmental event or disaster.

- Protection against interruptions or other disruptions of power supply in such a way as to ensure, as a minimum, the safe shutdown of critical information and communication systems (graceful shutdown). The power supply needs in these cases shall also be compatible with the elements identified in accordance with control measure 11.1.

The above requirements should apply and be ensured even if the organisation's equipment (all or part of it) is located in a third-party datacenter or in the cloud.
Identification and access tools (e.g. digital access cards, keys, access codes, etc.) must be in the possession of only those persons who are entitled to access such premises and must not be loaned to anyone else.

Documents that are located in offices should be adequately protected by measures to:

- Suitable filing cabinets that are locked with keys stored away from the cabinet; or
- locked safes.

,

# 10. DATA PROTECTION

## PURPOSE

The organisation implements a personal data protection policy and self-assessment with the aim of better compliance with relevant legal and regulatory requirements and greater protection of data subjects and the organisation.

## CONTROL MEASURE 10.1

The organisation shall design, implement, adopt and publish a Personal Data Protection Policy based on the general GDPR regulation.

## DESCRIPTION

The organisation shall carry out a self-assessment on personal data and on the compliance with the relevant provisions of the legislation. The self-assessment may be carried out using an appropriate methodology developed by the organisation or by an appropriate reliable external source.

The following sources are indicative:
https://www.dataprotection.gov.cy/dataprotection
dataprotection.nsf/page3a_gr/page3a_gr?opendocument
European Union Agency for Cybersecurity (ENISA):
https://www.enisa.europa.eu/risk-level-tool/risk
European Data Protection Board - Guide to personal data protection for small businesses:
https://edpb.europa.eu/sme-data-protection-guide/home_en

The self-evaluation process will be repeated annually.

The organisation shall keep the results of the self-assessment and implement any measures that are found to be necessary to ensure compliance with the relevant requirements.

The organisation will establish a personal data protection policy which will be compatible with the requirements of the relevant legislation, regulations and directives of the Office of the Commissioner for Personal Data Protection, with the results of the self-assessment (as described above) and will contain at least the following elements:

- A brief description of the organisation's activities
- The full contact details of the organisation
- The contact details of the data protection officer
- The personal data (categories) processed by the organisation
- The source from which the personal data originate (in cases where they are not collected directly from the data subjects)
- The purposes and legal bases of the processing
- The legitimate interests pursued by the controller or a third party (in cases where the processing is based on a legitimate interest)
- The recipients (or categories of recipients) of the personal data

- The period of retention of the personal data or, if not possible, the control measures used to determine this period
- Indication of whether personal data are transferred to a third country or international organisation
- Information on the rights of the data subjects (e.g. right of access, rectification, erasure, etc.)
- The existence of the right to withdraw consent (in cases where processing is based on the data subject's consent)
- Information on how data subjects can lodge complaints either with the organisation or directly with the supervisory authority.
- Whether the data subject is obliged to provide the personal data and what the possible consequences of not providing such data would be
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information on the logic followed and the relevance and envisaged consequences of such processing for the data subject.

More information can be obtained on the data protection/privacy policy/data subject information policy on the website of the Office of the Data Protection Commissioner in the part "Information for citizens" - "Your rights" - "Transparency - Right to information": https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/39B375E9A0126F47C22582F9002BFE2B

-

The personal data protection policy will be available as a minimum via the organisation's website and will be reviewed for appropriateness at least once a year.

# 11. OPERATIONAL IMPACT ANALYSIS

## CONTROL MEASURE 11.1

The organisation has designed and implemented an appropriate methodology for operational impact analysis. The results and key metrics resulting from the application of the methodology are recorded, maintained and feed into the design of relevant measures and implementations.

### PURPOSE

The organisation conducts a business impact analysis to identify in an organised way the priorities, levels and dependencies of its services and processes. Through this analysis, the organisation is able to adapt the various measures to its business requirements.

## DESCRIPTION

Operational impact analysis helps the organisation to identify and document critical operational processes and their supporting elements. This helps the organisation in understanding its environment and what is most important to it before taking steps to protect it. The operational impact analysis highlights how these key processes and services would be affected if normal operational functioning was impeded, interrupted or eliminated.

By implementing the methodology for operational impact analysis the organisation manages to:

- identify key operational processes and functions
- prioritise key operational processes and functions
- draw up a detailed list of requirements for recovery
- determine the impact that an outage will have on daily operations for different periods of the outage
- determine the maximum amount of time a process or service can tolerate being down (Maximum Acceptable Outage - MAO)
- determine the desired recovery time objective (RTO) in the event of a disturbance
- determine the minimum data age to ensure effective recovery (RPO - Recovery point objective)
- determine the financial, operational and legal impact that the organisation will have from a disruption affecting services.

The results on RTO (recovery time objective), RPO (Recovery Point objective) and MAO (Maximum acceptable Outage) will be used for decision making and design of relevant policies and measures (e.g. control measure 5.1.). In addition, the organisation shall create and document within the BIA the ways in which it will achieve the above metrics in the event of a disruption.
The relevant business impact assessments will be reviewed annually and in the event of significant changes in the organisation, such as office moves, mergers and acquisitions or the introduction of new services or a change of services.

**Disclaimer**

This document aims to support SMEs in achieving a minimum level of cybersecurity. The information provided is of a guidance nature and is not tailored to the specific situation of any individual or legal entity. This cyber-health framework does not constitute a legal commitment. Although the implementation of the proposed Cyber-Hygiene Framework enhances the level of cybersecurity, it cannot ensure that the business through the implementation will entirely prevent any cyber-attack. Any use, reproduction, disclosure, copying, falsification, adaptation or any other use of this document is prohibited without the prior written consent of the Digital Security Authority for this purpose.

Co-funded by the European Union's Digital Europe programme under grant agreement no. 101101331.

Co-funded by the Digital Security Authority (DSA)