Access control policy and procedures template

This maricopa county template aims, from the ground up, to help organizations manage the risks of managing user accounts, enforce and control access, separate duties, and remote access by creating an access control program. [The name of the organization] identifies specific requirements for protecting information and information systems from unauthorized access. [The name of the organization] will effectively report on the need to monitor access to the information and information system. 2 The purpose of information security is to protect information against unintentional or malicious disclosure, modification or destruction. Information is an important and valuable asset from [the name of the organization] that must be carefully managed. All information is valuable to the organization. However, not all of this information has equal value or requires the same level of protection. Access controls are put in place to protect information by controlling who has the right to use different information resources and by protecting against unauthorized use. Formalities must control how access to information is made available and how this access is changed. This policy also sets a standard for creating, protecting and changing passwords. 3 The scope of this policy applies to all [organization name], committees, departments, partners, organization staff (including system support staff with access to distinctive administrative passwords), contractual third parties and organization agents with any form of access to [organization name] and information systems. 4 Rules and procedures for controlling access to the definition are required to regulate who has access to information resources or systems [the name of the organization] and associated access privileges. This policy applies at all times and should be adhered to whenever [the organization's name] information is accessed in any form, and on any device. 5 Business information may sometimes be disclosed or accessed prematurely, by mistake or illegally. Individuals or companies, without proper authorization and clearance, may intentionally or accidentally obtain unauthorized access to business information that may adversely affect the day-to-day business. This policy aims to mitigate this risk. Failure to comply with this policy can have a significant impact on the efficiency of the organization's operation and may result in financial losses and inability to provide the necessary services to our clients. 6 Application Policy – Passwords 6.1 Password selection is the first line of defense for our ICT systems and helps together with the user ID to prove that people are the ones who claim to be. The password that is selected or misused is a security risk and may affect the confidentiality, safety or availability of our computers and systems. 6.1.1 Weak and strong A weak password is a password that is easily detected or detected by people who aren't supposed to know it. Examples of weak passwords include words selected from the dictionary, children's and pet names, car registration numbers and simple patterns of letters from the computer keyboard. A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and are difficult to work out even with the help of a computer. Everyone should use strong passwords with a minimum of at least seven characters. Contains a combination of alpha and digital, with at least one number more complex than a single word (these passwords are easier for hackers to crack). [Modifying the above as required to meet local needs] the organization recommends using environ passwords with the following form: static, vowel, cons, cons, cons, cons, vowel, vowel, vowel, cons, cons, number, number. Below is an example for illustration purposes: 6.2 password protection is critical to keep your password protected at all times. You must adhere to the following guidelines at all times [modify the list as appropriate]: Never disclose your passwords to anyone. Never use the password remembering function. Don't write or store your passwords where they are open for theft. Do not store your passwords in a computer system without encryption. Do not use any part of your username within your password. Do not use the same password to access different systems [organization name]. Do not use the same password for systems inside and outside the work. 6.3 Changing passwords must change user-level passwords at the maximum every 90 days, or whenever a system asks you to change them. You must also change default passwords immediately. If you become aware or suspected, that your password has become known to someone else, you should change it immediately and report your concern to [department name - for example, IT Help Desk]. Users should not reuse the same password within 20 password changes [edit as appropriate]. 6.4 System management standards password management process for individual [organization name] systems is well documented and available to selected individuals. All IT systems [enterprise name] will be configured to enforce the following: authentication of individual users, not user groups - no public accounts. Protection for retrieving passwords and security details. Monitor system access and login - at the user level. Manage the role so that tasks can be performed without sharing passwords. Password management processes must be properly controlled, secure and audited. 7 Policy application must be documented - Access to employee 7.1 official user management procedures for user access control, implementation and date to date to date for each application and information To ensure authorized user access and prevent unauthorized access. All stages of the user access life cycle must cover, from the initial registration of new users to the cancellation of the final registration of users who no longer need access. It must be agreed upon by [the name of the organization]. Each user must be granted access rights and permissions to computer systems and data that: fit the tasks they are expected to perform. You have a unique login that is not shared with or disclosed to any other user. You have a unique password associated with each new login. The number of people who have been forced to flee their villages has been reduced to more than 1,000. System management accounts must be provided only to users required to perform system management tasks. 7.2 You must first submit an application for access to the organization's computer systems to [a management name , such as the Information Services Assistance Office] for approval. Access requests must only be submitted if approval is obtained from [role name — for example, your administrator]. When an employee leaves the organization, his access to computer and data systems must be suspended when work closes on the employee's last working day. It is the responsibility of [the name of a role — for example, your responsible manager] to request a suspension of access rights via [department name — for example, information services assistance office]. 7.3 User responsibilities are the responsibility of the user to block their user ID and the password is used to obtain unauthorized access to enterprise systems by: following the password policy data described above in Section 6. Make sure that any computer they use is left unattended or logged out of it. Leave anything on the screen that may contain access information such as login names and passwords. Notify [section naming — for example, information services assistance office — and any related roles] of any changes in its role and access requirements. The use of modems on unowned personal computers of the organization connected to the organization's network can seriously compromise network security. You should not interfere with normal network operation. Specific approval must be obtained from [management name - such as information services] before any equipment is connected to the organization's network. 7.5 User authentication for external communications where remote access to the [enterprise name] network requires, an application must be provided via [department name - e.g. IT Assistance Office]. Remote access to the network must be secured by a two-factor authentication consisting of a user name and another component, for example, [the name of a related authentication code]. For more information please refer to [name of relevant policy - likely to be Labour policy. 7.6 Remote resource access to partner organization network agencies or third-party suppliers should not be given details of how to access the organization's network without permission from [management name – for example, IT Assistance Office]. Any changes to the vendor's connections should be sent immediately to [department name - for example, IT Help Desk] so that access can be updated or stopped. All permissions and access routes must be controlled by [department name - for example IT help desk]. Third-party partners or suppliers must contact [department name — for example, IT Help Desk] before connecting to the [organization name] network and must maintain the activity history. The remote access program should be disabled when it is not in use. 7.7 Os access to access control to operating systems is controlled by a secure login process. The specified access control must be applied in the User Access Management Section (Section 7.1) and the Password Section (Section 6) above. You should also protect your login procedure by: Do not view any previous login information such as the username. Determine the number of unsuccessful attempts and secure the account, if it is exceeded. Password characters are hidden by icons. View a general warning notice that only allows authorized users. All access to operating systems is via a unique login ID that will be audited and can be returned to each individual user. The login ID should not give any indication of the level of access it provides to the system (such as management rights). System administrators must have individual administrator accounts that will be recorded and audited. The administrator account should not be used by individuals for normal daily activities. 7.8 Access to applications and information within software applications must be restricted by using the security features included in the individual product. [Department name — for example, it help desk or 'employer'] of the program application is responsible for granting access to information within the system. [List modification as appropriate]: Must be compatible with user access management section (Section 7.1) and password section (Section 6) above. Be separated into clearly defined roles. Give the right level of access required for the user role. Can't be overridden (with administrator settings removed or hidden from the user). Be free of change from the rights inherited from the operating system that can allow higher unauthorized levels of access. Be registered and subject to scrutiny. 8 Compliance with the policy if it is found that any user has violated this policy, may be subject to disciplinary action [the name of the organization]. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the perpetrator (the perpetrators). If you don't understand. From this policy or how it can apply to you, seek advice from [the appropriate section name]. 9 Policy management determines the following table who is responsible, responsible or adviser under [the name of the institution] in relation to this policy. The following definitions apply: Responsible - the person responsible for the development and implementation of the policy. Responsible - the person who has absolute accountability and authority for politics. Consultant - person, person or groups that must be consulted before implementing the final policy or amending it. Information - The person, people or groups that will be notified after the policy is implemented or modified. The administrator [includes the appropriate function - e.g. Head of Information Services, Head of Human Resources, etc.] (c) Responsible [appropriate job inclusion - such as section 151 officer, finance manager, etc. It is important that only one role be held accountable.] [Inclusion of appropriate job title, management or group - such as policy management, staff teams, unions, etc.] informed [inclusion of the appropriate function, management or group - for example all employees of the organization, all temporary staff, all contractors, etc.]