NEVADA CLOUD

SECURITY POLICY

Table of Contents

1. INTRODUCTION

1.1. Purpose

This Security Policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in the company. Its goal is to protect the company and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

1.2. Scope

This document applies to all the users in the company, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory.

1.3. History

Version	Description	From	To	Author
1.2	Updated version	1/3/2019	28/2/2020	R. Meyer-Wilson

1.4. Responsibilities

Roles	Responsibilities
Chief Information Officer	• Accountable for all aspects of the company's information security.
Information Security Officer	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Information Owners	• Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
IT Security Team	• Implements and operates IT security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

1.5. General Policy Definitions

1. Exceptions to the policies defined in any part of this document may only be authorized by the Information Security Officer. In those cases, specific procedures are in place to handle request and authorization for exceptions.
2. Every time a policy exception is invoked, an entry is entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed.
3. All the IT services are used in compliance with the technical and security requirements defined in the design of the services.
4. Infractions of the policies in this document will lead to disciplinary actions. In some serious cases they could even led to prosecution.

2. IT Assets Policy

2.1. Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in the company.

2.2. Scope

The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

2.3. Policy Definitions

1. IT assets are only used in connection with the business activities they are assigned to and / or authorized to.
2. All the IT assets are classified into one of the categories in the company's security categories; according to the Specific business function they are assigned to.
3. Every user is responsible for the preservation and correct use of the IT assets they have been assigned. This is overseen and checked by the ISO (Information Security Officer).
4. All the IT assets are secured in locations with security access restrictions and layout according to the security classification and technical specifications of the aforementioned assets.
5. Active desktop and laptops are secured if left unattended. This policy is automatically enforced.
6. Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service is done through the approved Service Request Management and Access Management processes.

7. All personnel interacting with the IT assets have the proper training and are aware of the controls and security processes.
8. Users shall maintain the assets assigned to them clean and free of improper use. They may not drink or eat near the equipment.
9. Access to assets in the company's location are restricted and properly authorized, specifically those accessing remotely. Company's laptops, tablets, cellphones and other equipment used at external location is periodically checked and maintained.
10. The IT Technical Team is solely responsible for maintaining and upgrading configurations. No other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
11. Special care is taken for protecting laptops, tablets, cellphones and other portable assets from being stolen. Special precaution is taken in cases of extreme temperatures, magnetic fields and falls.
12. When travelling by plane, portable equipment like laptops, tablets and cellphones remains in the users' possession as hand luggage.
13. Encryption and erasing technologies as prescribed by POPI and EUGDPR standards and procedures are implemented in portable assets as protection in case of theft.
14. Losses, theft, damages, tampering or other incidents related to assets that compromises security are reported as soon as possible to the Information Security Officer.
15. Disposal of the assets are done according to the specific procedures for the protection of the information. Assets storing confidential information is physically destroyed in the presence of the Information Security Officer. Assets storing sensitive information are completely erased in the presence of an Information Security Officer before disposing.
16. All Paper documents that are disposed of are shredded by means of a confetti cross shredder and no other means.

3. ACCESS CONTROL POLICY

3.1. Purpose

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in the company.

3.2. Scope

This policy applies to all the users in the company, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

3.3. Policy Definitions

1. All systems that handle confidential, valuable, sensitive or personal information are protected with password-based access control.
2. An access control list is in place to control the access to resources for different users.
3. Access is granted under the principle of “less privilege”, i.e., each individual receives the minimum rights and access to resources needed for them to be able to successfully perform their functions.
4. Users are monitored in order to prevent them from trying to tamper or evade the access control in order to gain greater access than they are assigned.
5. Automatic controls, scan technologies and periodic revision procedures are in place to detect any attempt made to circumvent controls.

4. Password Control Policy

4.1. Purpose

The Password Control Policy section defines the requirements for the proper and secure handling of passwords in the company.

4.2. Scope

This policy applies to all the users in the company, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

4.3. Policy Definitions

1. All systems that handle confidential, valuable, sensitive or personal information are protected with a password-based access control.
2. Every user has a separate, private identity for accessing IT network services.
3. Identities are centrally created and managed. Single sign-on for accessing multiple services is enforced.
4. Each identity has a strong, private, alphanumeric password to be able to access any service. They are a minimum of 8 characters long, one capital, one numerical and one special character.
5. Each regular user may use the same password for no more than 365 days and no less than 3 days. The same password may not be used again for at least one year.
6. Use of administrative credentials for non-administrative work is prohibited. IT administrators have two sets of credentials: one for administrative work and the other for common work.
7. Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
8. If ever a password is deemed compromised, it is changed immediately.

9. Identities are locked if password guessing is suspected on the account.

5. Email Policy

5.1. Purpose

The Email Policy section defines the requirements for the proper and secure use of electronic mail in the company.

5.2. Scope

This policy applies to all the users in the company, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

5.3. Policy Definitions

1. All the assigned email addresses, mailbox and cloud-based storage and transfer links are used only for business purposes in the interest of the company.
2. Use of the company resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the companies' business is strictly forbidden.
3. In no way may the email resources be used to reveal confidential or sensitive information from the company outside the authorized recipients for this information.
4. Using the email resources of the company for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely forbidden.
5. Use of the company email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account is deactivated according to established company policy and procedures.
6. Users have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed necessary.
7. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is enforced. Only the Information Security Officer may approve the interception and disclosure of messages.
8. Identities for accessing company email is protected by strong passwords. The complexity and lifecycle of passwords are managed by the company's procedures for managing identities. Sharing of passwords is discouraged. Users may not impersonate another user.
9. Outbound messages from company users have approved signatures at the foot of the message.
10. Attachments are limited in size according to the specific procedures of the company. Whenever possible, restrictions are automatically enforced.

11. The use of Digital Rights technologies is enforced for the protection of contents.
12. Scanning technologies for virus and malware is in place in client PC's and servers to ensure the maximum protection in the ingoing and outgoing email.
13. Security incidents are reported to the ISO and handled immediately according to the Incident Management and Information Security processes. Users may not try to respond by themselves to security attacks.
14. Company mailboxes content is centrally stored in locations where the information is backed up and managed according to company procedures. Purge, backup and restore is managed according to the procedures set for the IT Continuity Management.

6. Internet Policy

6.1. Purpose

The Internet Policy section defines the requirements for the proper and secure access to Internet.

6.2. Scope

This policy applies to all the users in the company, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

6.3. Policy Definitions

1. All users have Limited access to Internet.
2. The use of Messenger services are only permitted for business purposes.
3. Access to pornographic sites, hacking sites, and other risky sites is strictly forbidden.
4. Downloading is a privilege only assigned to users authorized by the ISO.
5. Internet access is for business purposes only. Personal navigation is not allowed.
6. Inbound and outbound traffic is regulated using firewalls in the perimeter. Back to back firewall configurations are applied.
7. In accessing Internet, users behave in a way compatible with the prestige of the company. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
8. Internet traffic is monitored at firewalls. Any attack or abuse must be promptly reported to the Information Security Officer.
9. Measures are in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

7. Antivirus Policy

7.1. Purpose

The Antivirus Policy section defines the requirements for the proper implementation of antivirus and other forms of protection in the company.

7.2. Scope

This policy applies to servers, workstations and equipment in the company, including portable devices like laptops, tablets, cellphones and other equipment that may travel outside of the company facilities. Strict policies apply to external computers and devices accessing the resources of the company.

7.3. Policy Definitions

1. All computers and devices with access to the company network have an antivirus client installed, with real-time protection.
2. All servers and workstations owned by the company or permanently in use in the company facilities have approved, centrally managed antivirus protection. That also includes travelling devices that regularly connect to the company network or that can be managed via secure channels through the Internet.
3. Traveling computers from the company that seldom connect to the company network have installed approved antivirus protection.
4. All the installed antivirus applications automatically update their virus definitions. They are monitored to ensure successful updating is taken place, and latest version is installed.
5. Visitors computers and all computers that connect to the company’s network are required to stay “healthy”, i.e. with a valid, updated antivirus installed.

8. Information Classification Policy

8.1. Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the company information.

8.2. Scope

This policy applies to all the information created, owned or managed by the company, including those stored in electronically, cloud-based storage, and those printed in paper.

8.3. Policy Definitions

1. Information owners ensure the security of their information and the systems that support it.
2. The Information Security Officer, and management is responsible for ensuring the confidentiality, integrity and availability of the company's assets, information, data and IT services.
3. Any breach is reported immediately to the Information Security Officer. If needed, the appropriate countermeasures are activated to assess and control damages if any.
4. Information in the company is classified according to its security impact. The current categories are: confidential, sensitive, shareable, private and public.
5. Information defined as confidential has the highest level of security. Only a limited number of persons have access to it. Management, access and responsibilities for confidential information is handled with special procedures defined by Information Security Officer and management.
6. Information defined as sensitive is handled by a greater number of persons. It is needed for the daily performing of jobs and duties but is not shared outside of the scope needed for the performing of the related function.
7. Information defined as shareable can be shared outside of the limits of the company, for those clients, organizations, regulators, etc. who acquire or should get access to it.
8. Information deemed as private belongs to individuals who are responsible for the maintenance and backup of that information.
9. Information defined as public can be shared as public records, e.g. content published in the company's public Web Site.
10. Information is classified jointly by the Information Security Officer and the Information Owner.

9. Remote Access Policy

9.1. Purpose

The Remote Access Policy section defines the requirements for the secure remote access to the company's internal resources.

9.2. Scope

This policy applies to the users and devices that need access to the company's internal resources from remote locations.

9.3. Policy Definitions

1. In order to gain access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be requested only by the manager responsible for the information and granted by the ISO.
2. Only secure channels with mutual authentication between server and clients is available for remote access. Both server and clients must receive mutually trusted certificates.
3. Remote access to confidential information is not allowed. Exception to this rule may only be authorized in cases where is strictly needed.
4. Users may only connect from public computers when the access is for viewing public content.

10. Outsourcing Policy

10.1. Purpose

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions and processes.

10.2. Scope

This policy applies to the Organization; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

10.3. Policy Definitions

1. Before outsourcing any service, function or process, a careful strategy is followed to evaluate the risk and financial implications.
2. Whenever possible, a bidding process is followed to select between several service providers.
3. In every case, the service provider is selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
4. Audits are planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If the company has not enough knowledge and resources, a specialized company will be hired to do the auditing.
5. A service contract and defined service levels must be agreed between the company and the service provider.
6. The service provider must get authorization from the company if it intends to hire a third party to support the outsourced service, function or process.

11.ANNEX

11.1. Glossary

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An IT service provider that is part of a different organization from its customer.
Identity	A unique name that is used to identify a user, person or role.
Information Security Policy	The policy that governs the organization's approach to information security management
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.

Table 1. Glossary.