Internet Security Policy

Effective Date : 01/08/2013

Review Date : 18/07/2013

Approved by : Bhutan Telecom

Approval Date: 19/07/2013

PURPOSE

The DrukNet Internet security policy establishes the requirements to ensure that security policies remain current as business and technological needs evolve. This policy must be published and communicated to the staff of Bhutan Telecom and all the customers of DrukNet services.

SCOPE

This security policy serves as the minimum requirements that all Internet-related customers must adhere to. Policy statements addressing specific areas of Internet security are also listed. These policies cannot be altered by any informal practice or by commands of supervisors or managers without the prior information and approval of the management of Bhutan Telecom.

POLICY

Overview

1. DrukNet's assets and services must be appropriately used and protected against unauthorized access, disclosure, alteration or denial and security measures must be in place to ensure data integrity, authority, accessibility and availability. The responsibility of protecting DrukNet resources on the Internet is the responsibility of DrukNet staff. However, the responsibility also falls on DrukNet customers to protect their personal computers and other devices that are connected to the network provided by DrukNet. Additionally, both DrukNet staff and DrukNet customers must comply with the security policy implemented by DrukNet.

2. Customers of DrukNet services must adhere to the DrukNet Internet security policy and protect DrukNet assets with which they are entrusted and make appropriate use of these services.

3. It is the responsibility of the Security team, DrukNet to lead and implement security policies and provide security awareness to the customers. The Security team must also represent DrukNet in security forums and other related events.

Internet Security Policy

Acceptable Use Policy

DrukNet is committed in protecting its services and resources from malicious attacks and illegal actions, which may or may not be intentional. The Security Team, DrukNet will ensure effective security, given the active participation and support of every customer of Internet-related services. Therefore, customers must be aware of this policy and conduct their activities in adherence with this policy.

1. User Responsibilities

Basic Security Measures

All network users are responsible for implementing the following basic security measures with respect to their workstations:

- Installing a current version of antivirus software;
- Running an operating system that has been recently updated and patched;
- Utilizing a personal firewall is recommended;
- Users of DrukNet's Virtual Private Network or Wireless Network must implement antivirus software, an updated and patched operating system, and a personal firewall;
- Encrypting laptop computers and other mobile devices containing confidential information in accordance with the Mobile Device Security Policy.

2. General Use and Ownership

DrukNet may conduct audits on its computing assets to ensure compliance with this policy, that is, authorized staff of DrukNet may, within their capacity and capacity of available tools, monitor equipment, systems and network traffic at any time for the purposes of security, network maintenance and policy compliance.

3. E-Mail Service

3.1. Authorised staff of DrukNet may read the contents of DrukNet customer's e-mails for a variety of reasons relative to security.

3.2. DrukNet will attempt to provide maximum virus protection for all inbound and outbound emails. However, on detection of an infected e-mail, the virus protection scheme will attempt to clean it, or the entire e-mail may be deleted. The customer shall be notified of such action via email sent by *security.druknet@bt.bt*

3.3. Customers must not open e-mail attachments from unknown and suspicious senders as they may contain malicious software popularly referred to as Malware.

4. Web Hosting

Webmasters of websites hosted at DrukNet:

4.1. Must not store passwords in clear text or in any easily reversible form

4.2. Do not store passwords within an application including developer backdoors

4.3. Must ensure that applications/content management systems' and plugins used are most current and bug free

Webmasters must refer the *Website Security Policy* for detailed policy statements for website security.

DrukNet, Security team retains the right to scan your website hosted at BT, for vulnerabilities and submit vulnerability scan report and it is the responsibility of site webmaster/owner to fix any bug or vulnerability in accordance to the recommendation provided and if it still found to be security threat to other applications/users, DrukNet retains the right to suspend or block the site.

5. Physical Security

DrukNet will ensure that IT equipment and information requiring protection will be placed in secure physical areas with appropriate security measures and access to authorized personnels only. Customers of DrukNet entrusted with DrukNet resources must also ensure physical security of these resources.

6. Wireless

This policy statement applies to all the customers who connect to DrukNet network through wireless connection.

6.1. Customers must make appropriate use of the service and equipment that they are entrusted with and take all precautions to prevent unauthorized access

6.2. Customers providing their own wireless equipment to connect to DrukNet services are responsible for damage, loss, theft, etc. cause due to the equipment.

7. Accounts and Passwords

Customers are assigned accounts for their specific use for DrukNet services. Passwords are required to ensure proper authority over various resources and services. Therefore, customers:

7.1. Are responsible for the security of their accounts

7.2. Are fully responsible for sharing their passwords

7.3. Must change their passwords from time to time

7.4. Must use passwords that cannot be used for password guessing attacks such as brute-force attacks and dictionary attacks

7.5. Passwords that have expired should not be reused

7.6. Must log off from their accounts after the use or when unattended for long duration

Unacceptable Use Policy

Any activity that violates the policy is prohibited and malicious intents can be subject to penalization, depending on the severity of damage as determined by the Security team at DrukNet. The following activities are considered as unacceptable use of DrukNet services:

1. Introducing malware into Internet using DrukNet services with malicious intent

2. Causing security breaches or disruptions in service delivery by means of unauthorized access, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information

3. Performing any form of network monitoring that will intercept data not intended for user's computer such as port scanning, etc.

4. Spoofing user credentials or security of any host, network or account

5. Causing an interference or denial of service to other workstations other than the user's own workstation

6. Using scripts or commands with the intention of causing interference or disruptions in Internet-related services

7. Creating and sending unsolicited e-mail messages such as spam mails that may compromise security in any aspect.

8. Attempting, in any way, to restrict, inhibit, interfere with, or degrade or deny service to any user, any host or any server on the Internet.

9. Violating the regulations, rules or policies applicable to any network, server, computer database, or web site that you access.

10. Unauthorized port scanning. Using or distributing devices used for compromising security, such as password gatherers or password guessing programs, decoders, encryption circumvention devices, packet sniffers, unauthorized keystroke loggers, analyzers, cracking tools, or Trojan Horse programs.

11. Engaging in harassment, whether through language, frequency, or size of messages.

12. Using an account at another service provider to promote DrukNet web site in an abusive manner.
13. Using DrukNet account or network connection to collect replies to messages sent from another provider, which violate these rules or those of that provider or to participate in an illegal scheme.

14. Accessing any other person's computer or computer system, network, software, or data without his or her knowledge and consent.

15. Automated or manual generation of network traffic to simulate hits to blogs or other web-sites for reasons other than the good-faith intention of an Internet user to visit a web site to purchase goods or services or to obtain information, or with the intent to promote an unrelated web site. Examples: Click Fraud, Referrer Log spamming, web-based comment spam.

Incidence Response

In cases of security incidents, customers must report security incidence to security section of DrukNet for immediate action. Depending on the severity of the incidence, the customer responsible for the incidence

1. must restore the affected service within a period determined by DrukNet

2. is liable to pay for the damage done to the service and/or to the other customers of the affected DrukNet service

3. Must pay for the DrukNet resources used if the customer is unable to restore the service by himself and requires relevant person(s) at DrukNet to do the job.

Internet Security Policy

Definitions

Brute-force Attack: In a brute-force attack, an unauthorized person attempts to log into a system by repeatedly trying out different password combinations. Locking-out the user after a predetermined number of failed attempts is the best deterrent to this type of attack.

Dictionary Attacks: In dictionary attacks, the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. Dictionary attacks refer to exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically performed with software instead of an individual manually trying each password

Malware: Malwares stand for malicious software that are developed for the purpose of doing some harm. Thus, Malware includes computer viruses, worms, Trojan horses etc.

Network Sniffing: Hardware and software normally used for monitoring and troubleshooting problems on the network could be used illegally to obtain data, or slow the network response time. This is network sniffing.

Pinged Floods: Pinging is generally used to ensure that a host computer is reachable across the network. Used illegally, the Ping program would flood the network by constantly pinging a workstation or server.

Virus
A Virus is a program or a piece of code capable that attaches to files and replicates itself repeatedly, and from one computer to another, causing malicious events while propagating.

Firewall
A set of related programs, that protects the resources of a private network from users from other networks.

Virtual Private Network (VPN)
A VPN is the use of telecommunication infrastructure to provide remote offices or individual users with secure access to the organization's Network

Wireless Network
A network in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path