

RESOLUTION NO. 2278

A RESOLUTION OF THE CITY OF SALISBURY, MARYLAND ADOPTING A VIRTUAL PRIVATE NETWORK USE POLICY TO DEFINE GUIDELINES AND RESTRICTIONS REGARDING THE USE OF REMOTE NETWORK AND SYSTEM ACCESS BY CITY OF SALISBURY EMPLOYEES

WHEREAS, the City Council finds that it is in the best interest of the City and its citizens that it adopt a policy which will provide all City employees with the guidelines and limitations for appropriate use of Virtual Private Network technology; and

WHEREAS, the City Council believes that the use of such technologies is necessary for the City to operate openly and efficiently; and

WHEREAS, the City Council also recognizes that, since there is a potential for employee abuse of such technologies, a personnel policy must be implemented which will identify acceptable employee use of the defined technology resources; and

WHEREAS, the City Council believes that it is in the best interest of the City to provide its employees with a clearly defined policy of acceptable technology use.

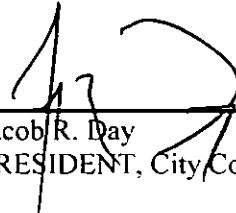
NOW, THEREFORE, BE IT RESOLVED that the Salisbury City Council adopts the attached Virtual Private Network Use policy.

THE ABOVE RESOLUTION was introduced and duly passed at a meeting of the council of the City of Salisbury, Maryland held on the 28th day of May, 2013 and is to become effective immediately upon adoption.

ATTEST:

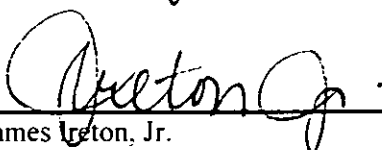


Kimberly R. Nichols
CITY CLERK



Jacob R. Day
PRESIDENT, City Council

Approved by me this 30th
day of May, 2013.



James Irton, Jr.
MAYOR, City of Salisbury

Memo

To: John Pick
From: Bill Garrett *BG*
Date: 5/17/2013
Re: Virtual Private Network Use Policy

Virtual Private Network Use Policy

The virtual private network use policy has undergone the following revisions before coming to its present state. The policy has been reviewed and approved by legal.

December 12, 2012

Section 2.2 modified at the request of Council to reflect that the approval of the Director of Information Technology is required for an employee to be granted access to the VPN system. Section 2.4 reworked to specify with greater detail the exact requirements that VPN enabled devices must meet in order to be granted access.

April 16, 2013

Section 3 modified to change 'intentionally' to 'negligently or intentionally', and to specify disciplinary action be taken in accordance with the employee handbook.

May 17, 2013

Minor grammar and capitalization issues were corrected.



Virtual Private Network Use Policy

Department of Information Technology

11/07/12 5/17/13

This document covers acceptable use of the City Virtual Private Network connection.

16 **1. Introduction**

17 The City of Salisbury (City) Virtual Private Network (VPN) provides a secure encrypted network
18 connection over the Internet between authorized City users and the network. The VPN offers secure
19 access for staff members who need to use information technology resources while they are away
20 from their offices or buildings.

21 **2. Guidelines**

22 The purpose of this document is to provide guidelines for Virtual Private Network (VPN) connections
23 to the City network resources.

24 2.1 City VPN does not provide Internet connectivity; it provides secure access into the City
25 Network. Individual users are responsible for selecting an Internet Service Provider (ISP),
26 coordinating installation, and installing any required software necessary for Internet Service.
27 Users of this service are responsible for the procurement and costs associated with acquiring
28 basic Internet connectivity including any associated service issues. VPN services work best over
29 broadband connections (cable or DSL). Use of dial-up Internet service is not recommended for
30 regular VPN activity, and due to high latency, satellite Internet services commonly will not be
31 able to establish a VPN connection.

32 2.2 VPN access will only be provided to City staff, and only with the approval of the
33 department head and the Director of Information Technology (IT).

34 2.3 VPN access is provided through a Microsoft server, requiring the remote access
35 computer to be Windows-based with the built-in Windows VPN client.

36 2.4 All computers, including personal computers, that will be connecting to the City's
37 internal networks via the City VPN must meet the following requirements prior to the IT
38 Department being contacted for configuration. The City periodically scans computers connected
39 to the City network to ensure compliance with the requirements below:

40 2.4.1 All computers must be behind a router or switch.

41 2.4.2 All computers must have an active Antivirus program which has been updated
42 within the past two weeks, and must be configured for automatic updates.

43 2.4.3 All computers must have all the latest operating system security updates,
44 patches and service packs installed, and must be configured for automatic updates.

45 2.4.4 All computers must be secured. A password must be required when logging into
46 the computer, or when the computer wakes from sleep, hibernation or screen-saver
47 mode. For personal computers, this password must be different from the City VPN
48 password used to access the system.

49 2.5 City VPN services are to be used solely for City business purposes. All users are subject to

50 auditing of VPN usage.

51 2.6 It is the responsibility of users with VPN privileges to ensure that unauthorized persons
52 are not allowed to access to City internal networks.

53 **3. Enforcement**

54 To maintain security, VPN services will be terminated immediately if any suspicious activity is found.
55 Service may be disabled until the issue has been identified and resolved. Any user found to have
56 negligently or intentionally violated these guidelines will be subject to disciplinary action in
57 accordance with the Employee Handbook.