INFORMATION TECHNOLOGY POLICY FOR **TSWELOPELE LOCAL MUNICIPALITY**

INCORPORATING
NETWORK USAGE & SECURITY,
END USER SUPPORT & ACCESS AND
ALL INFORMATION TECHNOLOGY
TRAINING ISSUES
Date 28 FEBRUARY 2014

TABLE OF CONTENTS:

7. DATA MANAGEMENT

8. ASSET MANAGEMENT

9. PATCH MANAGEMENT POLICY

Approval

DOCUMENT:	Information Technology Policy		
Copy Number:	**Master Copy**		
Compiled by:	K.A Mahase	**Reviewed by:**	
Compilation Date:		**Review Date:**	
Version:	Draft V 0.00	**Revision:**	
Distribution:	All	**Classification:**	
Document Release Approval		**Document Acceptance**	
Releasing Authority: Director: Cooperate Services	ICT Division	**Acceptance Authority:**	Council
Date Released:		**Date Accepted:**	
	Signature:		**Signature:**

INFORMATION TECHNOLOGY POLICY FOR TSWELOPELE LOCAL MUNICIPALITY

TERMS AND TERMINOLOGIES

The following are network policies that will be strictly enforced on all computers connecting to Tswelopele Local Municipality network and/or any other government network.

First the terms and terminology used in this document is defined:

TERM	DESCRIPTION
User	This is the person using the computer (PC) whether it is connected to the network or not. This is also the person who is responsible for the computer.
Network	A network is a state where all the computers linked together function to share information and services. The network is used to gain access to resources such as a mainframe, network file servers, Internet, modems, printers and scanners.
User ID	It is the ID or name a user is defined with on the network. It is a unique name and will not have a duplicate on the network.
IP Address	This is the address of a computer on the network and the Internet. This address is and should always be unique to allow access to the Internet and Intranets globally.
MAC Address	The physical and unique address of the network card installed inside the PC that an IP address can be assigned to.
Mainframe	A mainframe is a very powerful computer that does all processing ("work") on the mainframe itself. The mainframe is used to run applications and systems for use in the government that require high processor performance and storage space.

File server	A file server is a powerful computer used on the network running a network operating system enabling network users to access certain resources managed by the file server such as printers and hard disks.
HDD or Hard Disk	This is the permanent, magnetic storage media of a computer where data are stored and software applications installed.
IT	The acronym for Information Technology. Information Technology is the handling, management and distribution of information using technology that can be either electronic or manual and range from the spoken to the written word. In this sense however IT refers to the utilisation of technology commonly known as computers and related equipment and software.
Licensed Software	Software that has to be purchased and registered in the user's name or that of the organisation. Penalties can be applied if this is not adhered to.
Proxy Server	A server granting access to the Internet from a network workstation that can cache content for easier and faster access later on.
Cache	Information or data kept in temporary storage for easier and faster access later on.
Internet	A service that provides for the sharing of information on a global scale.
Intranet	A service where information are shared within an organisation or department relevant to that department or organisation but not available globally.

1. INTRODUCTION

This document dictates the use of the Tswelopele Local Municipality's network and access to it. It has the stability and security of the mentioned network on the agenda and will ensure that as far as possible all actions on the network are lawful, legal and just.
It also serves the community, the individual and the municipality as an entity.

The regulations listed here in will be regarded as binding on each individual member of the municipality, whether contracted, employed, hired on temporary basis or elected to office as per government laws.
No one is exempted from the rules and regulations here in that will in future be referred to as **the policy**, incorporating both user and network related issues, and will serve the mentioned municipality as a working document.

Any network support personnel that will take up employment with the municipality will adhere to this policy and where needed amend the policy to ensure that it stays in line with both national laws and international laws as far as Information Technology is concerned.
It is important to include international standards, as it will ensure that the minimum industry standards are adhered to.

The aim of this document is to ensure a stable, safe and secure networking environment that will indirectly serve the community of the Tswelopele Municipality in all its dealings.
The network should at all times be available and operational to ensure maximum usage of the network and resources on the network.

Changes hereto should be made after consultation with the Office of the Director of Corporate Services that is concerned with Information Technology and not without his/her explicit consent.
Any changes made to this document has to ensure that the organisation's main aims are adhered to and that no function is disabled or ignored.
All changes have to be committed to this document and the document has to be signed by the mentioned person or his/her delegated member in the head of the department's absence.

2. MANAGEMENT OF IT PERSONNEL

2.1 PURPOSE OF THE POLICY

The purpose of the policy is to ensure that the municipality has the necessary skills available to perform the necessary duties as expected in accordance with government laws.

2.2 HIRING OF PERSONNEL

2.2.1 All personnel should be hired in accordance with government laws and policies based also on the skills and experience of such people. People hired for especially Information technology work should also be trustworthy and able to perform such duties.

2.2.2 Where contractors are hired to perform duties the relevant laws should govern such as local business but also it should be verified that individuals employed by the relevant contracting company are trustworthy personnel and have the relevant experience and training as well.

2.3 TRAINING OF STAFF

2.3.1 The staff of the municipality should be given relevant training to ensure that tasks expected of them are performed effectively and without problems.

2.3.2 Desktop application training should be provided to all personnel of the municipality on the products they are supposed to use on the computers. The municipality should ensure that only the relevant products are used and that training is only provided on products authorised by the municipality. It would be recommended that all personnel on all desktop products used maintain an advanced level of skills.

3. NETWORK AND PC HARDWARE AND SOFTWARE

3.1 PURPOSE OF THE POLICY

The purpose of this policy is to govern the use of the network and computers or devices connected to the network as well as to inform of the legality of actions taken and what are expected of users and support staff.

3.2 SCOPE AND USAGE OF THE NETWORK

3.2.1 The network of Tswelopele Local Municipality is a government network as the municipality is a sphere 3 government institution. The network is to be **used for official purposes only** and no private work or data or illegal actions, things that are prohibited by national and international laws such as downloading movie files, music or software that is being pirated, is allowed on the network. This includes private downloads of movies, music in any format, software programs including games and other software for personal use and not for official purposes. None of these files may be kept on the network file server for sharing or made available on the network for any reason.

Should such files, data or programs, contain any viruses and or backdoors for outsiders to enter the network illegally, all costs incurred to rectify this problem may be recovered from the official responsible for such a breach. Responsibility and accountability for the contravention of international and local laws will be for the municipal manager and mayor if the perpetrator(s) are not known. If the perpetrator(s) are known then they will be held responsible and accountable for all actions taken and can the relevant punishment for the contravention of such a law be made applicable to the person.

3.2.2 All personal computers (PC's), notebook/laptop computers, workstations, personal digital assistants (PDA's), cellular telephone and any other device not specifically listed here with which one can gain access to the network to store, retrieve or access data or programs at Tswelopele Local Municipality are bound by this policy and the users there-of are bound by what this policy dictates. Not only is the user here-of bound by this policy but also by the National Intelligence laws and amendments there-of, laws prescribing government official's conduct

and laws governing the telecommunications and electronic communications of this country as well as international laws where applicable.
The network at Tswelopele forms part of a secure network within the government network where secrets are kept and should be kept to protect the people of this country against foreign invasions and or terrorism. It is therefore to be kept a secure network without outside network access and all actions on this network should adhere to the National Intelligence Agency laws and amended laws and regulations.

3.2.3 The network comprises the physical cabling, points, hubs, routers and file servers as well as the cabinets in which they are kept, i.e. all the hardware. Along with this the network also comprise of all the software installed and used on the network file servers and workstation also called personal computers, notebook/laptop computers and handheld devices mentioned earlier that run software paid for by the municipality and used in the general mandate of the municipality. All physical and virtual connections that are created for the purpose of communication via computer are deemed part of the network.

3.2.4 This policy includes all persons that are part of the Tswelopele Local Municipality as permanent employees, contractors or third party suppliers of services and temporary workers of the municipality.

3.2.5 No computer equipment (hardware) or software may be removed from the site without the consent of the relevant supervisor and/or Head of Department to ensure that the equipment and software are generally protected and safe at all times. The equipment may not be removed and used for private or personal use as it is the property of the local municipality and should be used in the service of the local municipality only and not to promote personal agendas.

3.2.6 No software that is licensed through the Tswelopele Local Municipality may be installed on any private personal computer (PC), notebook/laptop computer or any other type of computer or device that can use such software and be used to access data and/or the network.
All software can be used only for Tswelopele Local Municipality computers and installed on said computers. **These licenses should be kept and controlled by one person** that will issue only when software needs to be reinstalled or when a new computer has to be set up. All software used by the municipality must be recorded in a register and must be signed for when it is to be used by a support person for

installation. Software may not be taken off the premises without the authorisation of the Office of the Director of Corporate Service handling the Information Technology for the municipality. All software that must be issued for installation to the support person may only be issued with a reference number of a job card for such support or software installation. The relevant register must be presented at the annual audit and verified against the job card or copy there-of kept at the office.

The register aims to improve control over software and licenses as well as the installation of licensed software on computers. The licenses that have to be controlled are all software that are protected under US and/or international laws and treaties and that a certain premium has to be paid for. All illegal software must be removed from all official computers as soon as possible to ensure that the legally owned software only is installed on computers.

3.3 NETWORK ACCESS

3.3.1 All users of the network at Tswelopele Local Municipality must be registered users on the network and must be created as users of this network on the file server in either directory services or just the file server with a valid username and password. This will ensure control and effective problem resolution at all times. All users must have an allocated space on the file server where data can be saved individually or collectively as a group of users working on one File such as Finance. Only such data will be backed up regularly. This will also provide users with access to the network services available on the network.

3.3.2 The minimum rights assigned to all users will be Read rights and to Browse the network. Extra rights and privileges must be assigned only on request and where it is in the interest and explicitly necessary to have such rights.
No user should be allowed to have control over the network and or file server(s) at the office unless such a person was employed for that specific task. This will ensure better control and also make sure that the malicious intent is reduced.

3.3.3 Each computer has to have a marked network point in the office where the computer equipment is installed giving access physically to the network and network services available.

3.3.4 Physical access to the network server room and file servers is prohibited for all users except relevant support personnel appointed in writing. In the absence of such person or personnel a delegate should be appointed to perform minimum functions as and when required. This person should preferably be a computer support person or have relevant knowledge to perform such tasks, even on file servers as and when required.

3.3.5 Access to the network is guaranteed and available during all office hours from 07:30 to 16:00 daily. The network must be accessible from 06:00 to at least 18:00 daily. Any deviation to this must be discussed with the relevant Head of the Department responsible for Information Technology and authorisation must be obtained for such a deviation. Access to the network after hours should as far as possible be restricted and where possible totally avoided. This is for the sake of safety and network backups. Should files be open during backups it will not be backed up and data loss may occur.

3.3.6 All users must use a password with their usernames or user ID's to access the network. The password should consist of no less than six (6) characters without repeating such characters more than three (3) times. The password can be made up of any combination of letters and numbers. Passwords should also expire every thirty (60) days and old passwords may not be used for at least five (5) months.

3.3.7 A properly implemented directory service should be implemented on the network to ensure better security and safety of data and information. The directory should provide access to relevant network services and exercise control over such services.

3.3.8 All users must be granted at least one (1) network connection and not more than that. If more than one connection is allowed for a user to the network then it could mean defeating the security system. This will allow network user names to be shared and even logged in more than once, exploiting the network and services without being able to pinpoint the guilty party.

3.3.9 No user may use the network username of the network support person or of another user with more rights than himself or herself.

Where it is found that a user needs more rights he/she must apply for this from the Head of the Department responsible for Information Technology.

3.3.10 No user may use the **Administrator or Admin user accounts** or ID's to access the network. These accounts should be reserved for network administrators only and should also be controlled. The password of this account should be changed at least every thirty (30) days. **The password should be kept in an envelope with the Head of the Department responsible For Information Technology.** This account should only be used when necessary repairs are undertaken on the network and also when new implementations are to be done and the Administrator or Admin user account is necessary.

3.3.11 when a user leaves the employ of the municipality his/her user account must be locked on the last day of work. All official files or documents that user is the owner of must be copied to a location where it can be used and or updated. The relevant user account should then be deleted along with the user directory allocated to that user on the network file server.

3.3.12 When a user account is not accessed for a period of three (3) months that user account should be locked. When the user account is not used at all it should be deleted from the network and all files saved to a location where relevant personnel can access it.

3.3.13 All users should ensure that when they leave their workstations they log out from the network, especially if they will be leaving the workstation unattended for longer than ten (10) minutes. Especially where they access transversal systems or financial applications such as the SABATA FMS program. It is important to remember an unattended logged on workstation may be used by a malicious person to gain access to the network. Even visitors may cause irreparable damage to the network or a financial system or may access information that is confidential. All data on the network should however be considered as confidential, especially when visitors are visiting the office for any reason.

3.3.14 No person other than the person the computer was issued to may use it. Officials may allow access to another official for purposes like accessing and verifying programs and data. Private persons may under

no circumstances be allowed to use any computer or the computer network. Irrespective of the age and qualification of the person he/she may not access or use the computer.

3.3.15 All users will receive an Internet Protocol Address (IP Address) with which he or she can access the network and Internet. This IP Address is assigned permanently to the relevant user by assigning it to the relevant network card. This will ensure that the user has the relevant access he/she needs. When a network card becomes faulty care should be taken that the new network card should use the same IP Address. The faulty network card can then be sold or thrown away. Important to note is that there are companies and individuals that collect such cards and recycle it. This option can be explored to generate a revenue and use the funds where needed.

3.3.16 Users that will be away from work for long periods of time should inform the network support person to lock the user account so no one can gain access using that user account. This will ensure better security on the network and safety of all data on the file servers. The user can then request for unlocking the user account when returning to the office.

3.3.17 Where the municipality needs access to transversal systems at provincial and national levels provision should be made for this to occur effortlessly and security procedures are in place to ensure safety of data and applications. Only people that are registered and specifically granted access to such systems must be allowed to have the relevant software on their workstations/computers. The user account information and passwords should not be shared at all with any other member of the municipality regardless of rank, stature or designation. The person should not be hassled in any way to give such information as that person has undergone security checks where applicable and changes are registered on the system(s) against the user ID or account and the user will be held responsible for changes implemented on the system(s).

3.4 NETWORK SERVICES

3.4.1 Network services include all relevant and applicable applications that ensure the use and not abuse of the network. File services and printing services will be provided on the network as well as a backup service for official data and documents only. The saving of private data, applications and documents on the file server is strictly forbidden and will be removed without notification to the relevant owner. Although the individual has a right of privacy the file server is a public entity and environment that has to be respected and will only be used for saving official data and documentation. All documents saved on a file server, whether in a user allocated space or not will be deemed public property and can and will be removed from the server without notification to the owner of the file. There will be no privacy statements and/or claims of files saved on the file server.

3.4.2 Printing services are there for the explicit use of the municipality in the execution of the duties there-of according to the relevant laws and regulations. Private printing and printing of private and personal files, documents or data are prohibited and can lead to disciplinary action with regards to the abuse of government property and/or illegal contravention of network and government security. All users may use appointed printers and printer devices such as photocopiers that can perform the functions of a network printer. Printers to which restrictions have been added are deemed off limits to all except the persons appointed as users of that particular printer and/or printer device. One such occurrence may be printing to the colour laser printer.

3.4.3 All users on the network will receive a specified amount of space on the network file server where data may be stored. Such folders or directories are subject to regular audits and investigations and should contain only official data or work related information. All private and/or personal data with the exception of curriculum vitae (CV) are prohibited on the server.

3.4.4 The network provides every user with a valid Internet Protocol Address (IP Address). This address is sometimes linked to certain services and access options and should not be swapped out between users. Such addresses can be assigned dynamically via DHCP server or statically assigned on the workstation itself. Users should not use each

other's IP Addresses to gain access to certain services but should apply for access to such needed services via memorandum to the Office of the Director of Corporate Services responsible for Information Technology.

3.5 NETWORK AND PC SUPPORT

3.5.1 The appointed network support personnel should undertake all network support only and no user may interfere in such actions unless appointed to do so in writing by the Office of the Director of Corporate Service responsible for Information Technology. This is to ensure that where support contracts are running and paid for the municipality gets the relevant service from the provider. The service provider may refuse such work when there is interference from the client and this may cause disruption on the network.
When a support company is used there should be one person appointed to liaise with the company from the municipality and all actions should then flow via this person. This is to ensure responsibility and accountability for work done on the network. Where a person of the municipality becomes skilled in an area that could assist the provider he/she may be approached via the liaising person for such information to assist when such skills are not readily available. Care should be taken that the support provider does have the necessary skills or access thereto to perform all necessary duties in this regard. The support provider may escalate problems but care should be taken that trustworthy people are used and not potential network threats. If the municipality makes use of employed personnel the municipality must ensure that the relevant helpdesk and call support structures are in place. Care should be taken that a call that cannot be resolved locally be escalated to properly trained and trusted personnel and not to people that are known to exploit such instances.

3.5.2 All support must be performed against a logged call with the detail of the call that was logged. Such a call should then be attended to as per request and written off after resolution of the fault. A copy of the job card should be kept with the liaising personnel member to ensure that the work was performed to standard and satisfaction.

3.5.3 All network support should be given priorities and should be attended to immediately. All calls where all users are affected should be attended to immediately. A list with the priority work should be drawn up and attended in that order if and when it occurs.

3.5.4 It is the responsibility of the computer user to log any faults with the computer or the network that he/she may experience. Faults that are not logged will not be attended to and the network support personnel or service provider cannot be held responsible for such faults or problems. Faults mentioned to the support person verbally cannot be seen as an official logged call and a fault has to be logged irrespective of the response from the network support person or company. Faults attended to without a job card and official fault log can be deemed as free of charge and may not be paid for. The support person or provider should therefore ensure that all work he/she does are properly logged and documented.

3.5.5 No user, irrespective of his rank or stature are allowed to approach the support person directly when faults are logged through a helpdesk to ensure that favour are not part of the operation. As stated above only work that is logged will be and should be paid for.

No person may under any circumstances make use of the support person or Provider Company to repair privately owned personal computers during official times and have such bill be sent to the municipality. The only exception is where this was agreed to in the person's contract and this would be part of the person's benefits. All privately owned personal computers or devices are to be repaired outside of the contract with the municipality and would be for the account of the relevant person.
Should a company be used and they decide to provide a support person for private repairs as needed this must be done then outside of the agreement with the municipality and are for the account of the person himself/herself. A separate person and not the person allocated to perform the support duties for the municipality on the day should also do this. Where the municipality employs a person that person are not allowed to perform any private duties within official working hours, irrespective of the requester. That will include all members of the executive committee, councillors, the mayor or any other person that forms part of the municipality. Such a person may also not bring in private work to be performed during official working hours. Such actions will be seen as a contravention of the agreement or service contract.

3.5.6 Only recognised and appointed support technicians are allowed to work on computers of the Tswelopele Local Municipality. No other person, regardless of connection, stature, rank or qualification may work on any computer or computer equipment belonging to Tswelopele Local Municipality unless the problem was escalated to the person by either the support person or the Office of the Director of Corporate service responsible for Information Technology in writing and the escalation was favourably accepted.
Only work directly requested from the support person or company will be performed and no extra work may be done at all. For instance when both a software problem is experienced and a hardware problem both should be listed and reported. If this is not done only the reported problem or fault will be dealt with. If no job card exists for a fault experienced such a fault must first be logged before it is being attended to. This has to be done in order to assist in the recordkeeping of expenditure on computers and related equipment. No support task may be undertaken without such a job card.

3.6 NETWORK AND PC HARDWARE

3.6.1 As stated above all computer equipment that forms part of the network or that are used on the Tswelopele Local Municipality and that was paid for or donated to the municipality are the property of the local municipality. The equipment is there to provide certain services to the users on the network and to enhance the service of the municipality to the community.

3.6.2 None of the mentioned items may be removed individually or in-group from the site without the explicit consent of the Office of the Director of Corporate Service responsible for Information Technology. All network equipment is to remain on site unless the Office of the Director of Corporate Service responsible for Information Technology authorise such a move when necessary for repairs, replacement and/or reconfiguration. All other equipment may be removed with the consent of a delegated person but network equipment will not be part of this. If it is an emergency another Head of Department that is taking care of the duties in the absence of the appointed member should give authorisation. This is done to protect the network and services as well as data on all file servers.

3.6.3 No user irrespective the rank or stature is allowed to remove network cables from the network or server or even computer for use elsewhere. This can be seen as sabotage or theft to disrupt network services and are subject to disciplinary action against such a person. Theft will be subject to the relevant laws of the country for which jail terms may be applicable.

3.6.4 All computer equipment that are broken or fail as a result of rough handling and/or abuse can be recovered from the relevant person guilty of such an offence. Care should be taken in such proceedings that all relevant avenues have been explored to educate and train the person as to ensure that the safety of the equipment is priority.
Unnecessary rough handling is something that has to be checked into and abuse and abusive actions should be sternly reprimanded. If the user persist with this action the relevant steps should be taken immediately and such equipment should be taken away from that person, irrespective of his/her duties.

3.6.5 Theft of equipment should be reported to the relevant authorities and should be dealt with. Care should also be taken that security measures in place are adequate and that measures implemented are cost effective and efficient.

3.6.6 Where computer equipment have to be moved from one location to another the relevant information should be given to the support person involved at least thirty (30) days beforehand. This is to plan for any contingencies such as movement or installation of cables and also expansion of existing equipment. This can also provide time to acquire new equipment should this be necessary or the relocation of current equipment and the reconfiguration there-of. Reconfiguration of equipment is very important as to ensure that when the actual move takes place the items can be plugged in and will work without major disruptions in work.

3.6.7 Support personnel should be consulted on the purchase of new hardware to ensure that the new hardware can work with current hardware and also the network and network software and that the new hardware will not cause downtime on the network.

3.7 NETWORK AND PC SOFTWARE

3.7.1 All network and personal computer software installed on the file servers and personal computers acting as workstations on the network are deemed licensed and the property of Tswelopele Local Municipality. All privately owned software must be removed from such computers and file servers regardless of the use there-of. The Public Administrations Committee issued instructions that only official software is allowed to be on any government computer, regardless of the use there-of. Since this is also a government office such instructions must be adhered to in order to avoid further steps taken.

3.7.2 All computer software that are licensed and used at the municipality must be listed in a register and properly issued to a user. Licenses that are left over afterwards should be declared and not issued for private use or privately owned computers unless specific provision was made for such installation in a government law on national level. No local government laws may dictate such steps; as such registers must be subjected to national Treasury inquiries and inspections as well as that of the Auditor General. Failure to submit such registers may result in penalties and/or subpoena to give evidence before the Public Accounts Committee.

3.7.3 Only relevant, official software may be used and installed on computers. No games or any type of gaming software or activity pack or entertainment software may be installed on official computers. This instruction was given under Public Administrations Committee as to ensure improvement of work performance and better utilisation of especially computer equipment. That entails that even games that comes with the operating system are not allowed to be installed for any purpose. Training computers may have such software installed for reference and specific training only. Common complaints from public were that government officials spend more time playing computer games than attending to the needs of the public and the community as a whole. Regardless of whether the executive committee allows games on computers or not this statement should be taken into consideration as it reflects negatively on public officials and government as a whole.

3.7.4 All software that are planned to be installed or upgraded on the network must be communicated at least thirty (30) days in advance to the Office of the Director of Corporate Service responsible for

Information Technology. A proper project plan must be submitted as well as all downtime planned and the affected workstations of the municipality as well as how they will be affected. This will ensure timeous notification and planning can be done to overcome negative affects of downtime. This will also ensure that there is a continuation of services regardless of the downtime.

3.7.5 No BIOS or screensaver passwords are allowed on computers of the municipality unless it is stated that the relevant computer is a security risk and has to be protected. Such passwords should then be made available to the relevant Head of the department or office manager and used only in the absence of the relevant user if data is needed urgently from that computer.

3.7.6 The support personnel should be consulted before new software is purchased as system requirements should be adhered to and also network standards should be considered. In some cases newer software cannot work with already installed software off the shelf and relevant patches should be downloaded or obtained before such software is installed and implemented. Consulting the support staff will ensure that the matter is investigated and that all considerations are taken into account to lessen the downtime and ensure that there is no extra software and hardware needed for the software to work properly. The support personnel should also ensure that the network would not be negatively affected by the planned software's installation and usage. All systems should have windows update enable for regular updating of patches and updates to the system.

3.8 USERNAMES AND PASSWORDS

3.8.1 All users must have a proper username and a password that will grant them access to the network and network services available on the network. The name must be compiled in accordance with the naming standards that are authorised and agreed to for the network.

3.8.2 The username must be in accordance with standards used in all other government levels and departments to ensure a standardised network that can be easily managed and supported and that will adhere to policies and procedures from the National Intelligence Agency and relevant intelligence laws applicable to all levels of government and also organisations that are seen as key infrastructure for the government and the country.

One example is to use the surname of each person and the initials of the person. ***The first seven (7) characters of the surname*** is used and one initial, normally the first. If there is a duplicate username the second initial is used. If there is still a duplicate the whole surname is used or parts of the first name, not only the initial, until there is no duplicate username. In some cases it may be that the people have the same names and surnames and seniority can then be used to differentiate or a nickname by which one of the people is known may be used with the normal username make up. Only the initial should then be used to differentiate. Care must be taken that nicknames are not derogatory to a person or humiliate or offend that person but must be accepted by the person. Where possible however this must be avoided. Care should also be taken that the username does not exceed ten (10) characters as it may encounter problems on some systems and could create problems. ***The minimum password length must be six (6) character and the maximum twelve characters*** and should include alphabets and numerical characters.

3.8.3 No user may offer his/her username and password to any person, regardless of rank or designation, to access the network or any network resource available on the network. All users should subsequently be limited to have only one (1) connection to the server and all other network services. Only through application and permission given by the Office of the Director of Corporate Service responsible for Information Technology may more than one connection be granted to a user. No user may also use another user's user account (**username and password**) to gain access to the network for any reason. In such cases the user account must be locked and the case be reported to the relevant Head of Department. It may not sound serious but it was found in many other cases before that individuals using another person's user account committed fraud, corruption or sabotage and such cases had widespread repercussions. Therefore such measures are employed to prevent such actions rather than to cure the results of such actions.

3.8.4 No user is allowed to use the Administrator user account to gain access to the network unless the person has been appointed in writing as the network administrator and have completed the relevant courses in this regard. Accessing this account will give access to areas that should not be accessed by users and may lead to misconfigurations that could incapacitate the network and bring about unnecessary downtime on the network. Downtime that is brought about by users through either

intended and/or malicious actions may ensure that the users are charged for the support in order to repair such damage. Since this account has access everywhere on the highest levels contravention of this policy should be reported to the Office of the Director of Corporate Service relevant department whose member contravened the policy.

3.8.5 Where people leave the employ of the municipality they should be given the chance to remove any private and personal information from the computer and also ensure that data on the server is official data and not personal data. The user account must be locked for a period of thirty (30) days and e-mail received should be forwarded onto the new address provided. This period will also ensure that the relevant data is copied to the personnel that would need it and allow for the reallocation of personnel where applicable. After this time the user account should be removed from the file server and the system synchronised and updated to reflect the relevant changes.

4. INTERNET POLICY

4.1 PURPOSE OF THE POLICY

The purpose of the policy is to assist in the control of and access to the Internet and the publishing of information.

4.2 INTERNET USAGE

4.2.1 The use of the Internet is subject to the relevance of it to the employee's job function and work. The government does not allow access to sites that are not work related or that can degrade the service and image of the government locally, provincially or nationally. All Internet sites accessed must be work related as far as possible. The Internet should be used as a tool to promote the image and responsibilities of the municipality and to ensure that it can provide a better service to the whole community.

4.2.2 The government has through criticism and in some cases laws directed that the following sites are not to be accessed from government computers as to protect the government against such criticism:

- Web sites that contains nudity of any type (hard core, soft core, sex or other pornographic content not mentioned specifically, including so- called art oriented nudity).

- Web sites that promote or display any type of nudity, sexual actions and graphics of children and persons considered children under the laws of the country. Where this instruction is ignored the person opens himself/herself not only to departmental disciplinary action but also to criminal prosecution.

- Web sites that displays violence to promote violent behaviour or attempt to disgust and/or upset members of staff and the public visiting the offices.

- Web sites with content that promotes action against the government or organisations that are protected under government laws.
- Web sites that promotes propaganda against any person or group of persons that are protected by law.

- Web sites that seeks to discredit any organisation, statutory or private.

- Web sites that allows for the use of government computers to perform illegal actions such as distribute software or music and other similar sites where information is illegally shared over the Internet.

- Web sites that has the aim of illegally accessing the user's computer or gain network access where the user works.

- Web sites that enables the user to play games online and that will abuse available bandwidth to such an extent that the normal work of employees are negatively affected.

- Web sites where people can communicate socially over the Internet in chat rooms or using a client to enable such actions like MSN Messenger, Yahoo! Buddy, etc.

- Web sites that deals in illegal products or content. The management of the municipality has discussed and agreed that the use of the Internet for sites not belonging to any of the above-mentioned criteria and that is not work related will not be prosecuted provided that visiting such sites does not negatively affect the operation of the person and/or department. This is where Internet services are available at present. New installations will not be granted on the premise of accessing the Internet because of the above-mentioned statement. The government laws and direction should in all cases still be adhered to and applied to ensure good governance and control over government funds and time. Internet access will not be allowed where a job function does not allow such access.

4.2.3 Users of the Internet are not allowed to download music in any format, movies or any software that are deemed licensed software for personal use and or retail purposes. This is in direct contravention of copyrights and anti-piracy laws internationally and can open the official to criminal prosecution. No user may utilise government equipment for such actions. This includes using government issued compact disk rewriters (CD-RW) to reproduce music or movies for any reason, including but not limited to personal use or retail of such content. This will also include reproduction of such content for official use where no explicit authorisation was granted or obtained for the reproduction of such content to benefit the department or organisation. Where it forms part of a presentation that aims not to discredit but educate without contravening the copyright of such content but rather enhance the organisation or department without having the content as the main focus such content may be recorded for use by the relevant personnel only. Where such content is to be used publicly the necessary authorisation must be obtained for the use of such content.

4.2.4 Users with Internet access may not have any or all of the following applications installed on their workstations/computers as it abuse available bandwidth and can be used to defeat security systems and software in place:

- mIRC / Streaming of Internet Radio,TV Channels
- ICQ / MSN Messenger / Delicious
- Yahoo! Buddy& Messenger /Companion / Google Chat / You Tube
- MSN Messenger / Skype / Facebook
- AOL Companion / Bing / Twitter / My Space / Digg
- BonziBuddy / Bleet Box / Bebo
- Any other IRC-related application not mentioned here, except that which may be allowed by management that will be part of communication packages in place on the network such as a relay agent shipping with programs such as GroupWise, MS Outlook and MS Exchange. Such programs are guaranteed as secure communications by their owners and will not aim to defeat the security systems and software installed and implemented on the network. The mentioned applications have been found to carry intruders successfully into secure environments and can disrupt network operations and cause downtime or add to the distribution of computer viruses.

4.3 INTERNET PUBLISHING

4.3.1 All content to be published on the Internet must be authorised before it is published as information that are considered sensitive may result in public uproar and action against the department or municipality. No information may not be published without the authorisation of the office manager or his/her delegate.

4.3.2 The publishing of information on the Internet should be done only by one person or institution or company to avoid duplication of tasks and to ensure accuracy of information. This will ensure that only relevant information is published on the Internet and that information has been cleared through the relevant channels to be published. If outside personnel do the web publishing then it is imperative that one

person be appointed to liaise with the company, person or organisation responsible for publishing the information to ensure that all work done are according to the wishes of the municipality or department.

4.3.3 The publishers of information should ensure that the server being used is secure and properly protected against illegal outside access. No web page published on Microsoft Internet Information Server should be considered safe and extra precautions should be taken to safeguard the server against illegal outside access. The Internet Information Server and all upgrades there-of has been shown to have security issues and allow illegal access to the server and network.

4.3.4 The information that should be published and be publicly available according to government laws should be made available on the web page for all Internet users to see and access. This should also be published on the Intranet page to ensure that it is accessible to all.

5. ELECTRONICMAIL (E-MAIL) POLICY

5.1 PURPOSE OF THE POLICY

The purpose of the policy is to govern, control and assist in the use of electronic communications using electronic mail and to raise awareness of actions that is done using e-mail and the steps that can be taken in such instances.

5.2 E-MAIL USAGE

5.2.1 Electronic mail or e-mail should be seen as a privilege and not a right. It is therefore imperative that the user should ensure that his/her e-mail access is kept official and at all times devoid of profanity, obscene, racist, defamatory, abusive or threatening, discriminatory or otherwise biased remarks or content, lies to discredit the municipality or any individual that acts as representative of the municipality or government and propaganda to discredit any person or group of people or party in any way.

Municipal computer users should also not distribute or forward any content that is sexual, pornographic, biased, offensive or violent to disgust or that can be viewed as inappropriate or illegal content. The principles of good governance should at all

times be adhered to and practiced without exception. All e-mail messages that consist of files that are copyrighted and therefore illegally distributed via e-mail are deemed illegal and steps can be taken not only disciplinary but also in a court of law against offenders.

It is also illegal to send information that is derogatory to any person or messages of sexual harassment via e-mail to any person, either within the municipality or outside. It is also illegal to read any e-mail message intended for a specific person, unless specifically instructed or requested to do so. Where people allow other access to their e-mail messages it should be noted that permission is given to read messages received via e-mail and therefore it is not deemed illegal to read any message received.

People making use of proxy connections to other personnel's mailboxes should therefore rather be appointed in writing to accept and read e-mail on behalf of the person. It is also deemed illegal to send e-mail that contain user accounts and passwords to persons not on the network or not members of the network, especially if those accounts and passwords grant access to the network with administrator or equal rights and the intended party uses it illegally. When instructed to do so such information may be sent via e-mail but only on instruction by a member of senior management.

All users should note that in some cases the steps that can be taken include jail terms and such actions may be criminal and will be prosecuted to the fullest extent of the law as to show a no mercy towards public officials abusing the privileges they have at the work place and to show a firm stance against criminal elements in the community.

5.2.2 E-mail users should not distribute any e-mail that can harm the network of Tswelopele Local Municipality or any other government organisation or department or private network. Distributing such programs or content can be viewed as sabotage and relevant proceedings may be entered into against the person.

It is important to note that the government will under no circumstances protect an individual or group of individuals that do not adhere to the laws of the country or disobey any instruction, written or verbal, to ban certain activities or actions. People that do make themselves guilty of such actions will face

prosecution and may have to serve jail terms for such actions.

5.2.3 Users are allowed to use any e-mail client to send or receive information provided that the program is accepted and supported by technical support staff or the company employed to perform such tasks. The user should also note that only the authorised email clients will be supported and no other.

5.2.4 Users that distribute computer viruses via e-mail may be held responsible for charges in ridding the system of such computer viruses, especially if it was sent knowingly that such e-mail contained a computer virus or viruses.

5.2.5 E-mail should as far as possible not be allowed to accumulate on the file server as to conserve disk space and ensure proper use of the file server.

5.2.6 The municipality Internet Service Provider is required to keep e-mail and/or headers for a specified time. The timeframe is yet to be fixed and it could come down to the organization to hold such information for a specified period. This is required by law and should be considered when accumulating e-mail and other data on file servers. A formal instruction will be issued to inform of such actions to be taken. This will be in accordance with the intelligence and information availability acts of the country.

6. ANTI-VIRUS POLICY

6.1 PURPOSE OF THE POLICY

The purpose is to protect End-Users and Organisational data as well as critical Applications, and systems files from being corrupted, deleted or infected against malicious malware or software.

6.2 ANTI-VIRUS APPLICATIONS

6.2.1 The municipality should have in place an anti-virus strategy that will protect or aim to protect all computers on the network or connected to the network either via cable media or through wireless connections.

All computers should have anti-virus applications installed to guard against the threat of computer viruses. The strategy should include not only the file server but also all computers that connect to the network at Tswelopele Local Municipality.

6.2.2 All computers that connect to Tswelopele Local Municipality network should be protected against viruses and therefore regular updates should be made available and done on all computers at least once per week. This will ensure that the network is at all times operational where possible. It is impossible to guard against all computer viruses and when a virus threat is detected and the scope of the problem is too much for one person to handle he/she should be allowed to escalate the problem to contain the virus as quickly as possible. The quicker the response the more likely it will be that data corruption is limited and data protected against outside exposure and exploitation.

6.2.3 All e-mail that is received should be scanned for both spam mail and virus threats received via e-mail. This can be done at both the server and the workstation and should be used to ensure added protection of the network and the computers on the network.

6.2.4 Firewall software should be installed on all computers accessing the Internet or a similar remote network such as a bank's secure site where access to the site is not gained through the Internet connection hosted by the file server.

7. DATAMANAGEMENT

7.1PURPOSE OF THE POLICY

The purpose of the policy is to define and accurately control all data generated or input on the network. Although some of this may have been covered earlier it is still relevant to discuss under this heading.

7.2GENERATED AND INPUT DATA

7.2.1 All data that are input into any computer system using either a mouse, keyboard, microphone, scanner or any other input device is referred to as input data. This includes the data captured by scanner as

part of the document management system that is planned for the future for this office and other government offices around the country. All such

data are to be carefully captured and verified for correctness as to ensure that all information generated or derived from it is accurate and just.

7.2.2 Generated data is usually the result of captured or input data. This type of data is usually the sought after product when budgets are compiled and are dependent upon the input data. Both types of data should be protected by secure connections and firewalls and anti-virus software. Generated data may not be changed or altered unless the relevant input data was verified as captured incorrectly.

7.3 MANAGEMENT OF GENERATED AND INPUT DATA

7.3.1 All data is important to the municipality and should be verified as being correct before and during the capturing process and then also afterwards. This will ensure that data is correct and this will ensure that accurate data or information is generated.

7.3.2 All users should receive a specified amount of storage space on the file server where data can be kept that are work related under their own name. This directory or folder should be accessible to the user only and can contain all correspondence and work related information generated between him/her and the supervisor or municipality for whatever reason. It should however not contain any private files such as data or programs.

The municipality's Head of the Department responsible for Information Technology should decide upon the size of the directory where users may create, modify and erase data pertaining to themselves and the work. It is the user's prerogative on what he/she saves in this directory as long as private and personal information is kept from the server.

7.3.3 Along with user home directories all functions should receive a space on the file server where data specifically pertaining to that job function can be kept. Such directories should have the name of the relevant function such as Finance or Personnel or Stock Control depending upon the functions and be accessible to the members of that function only. Only one or two people in such a function should receive rights to delete files from the directory or folder but all should be able to

create new files, change the content there-of, view all the files and be able to generate output. These directories must contain data only pertaining to the function and not individuals unless data is generated in the name of an individual but it is applicable to the whole function. No private or personal data or programs may be kept in this directory.

7.3.4 A general directory or Website must be setup to publish data relevant to the whole municipality such as circulars for jobs, functions and new policies or general feedback to staff. Such a directory should be updated regularly and should only
contain information relevant to all members of the municipality and should not contain personal or private data or programs. An Intranet will provide the function of feedback and keep the members of the municipality informed of work related issues
and policies as well as social events and gatherings.

7.3.5 All data should be regularly backed up and it is advisable that data be kept for a period of at least 3 months off site for disaster recovery. A full backup should be done at least once per week with differential backups done daily to ensure that all data are properly backed up and that data can be restored if and when needed.

8. ASSET MANAGEMENT

8.1 PURPOSE OF THE POLICY

The purpose of the policy is to assist in governing and controlling assets specifically in respect to Information Technology and to guide in the management of such assets.

8.2 USAGE OF INFORMATION TECHNOLOGY ASSETS

8.2.1 All equipment and software that are used in Information Technology are seen as assets to the municipality and must be properly managed and controlled to ensure optimum usage of such equipment. All Information Technology and Information Technology related assets should be controlled according to relevant laws, policies and instructions governing the control of such equipment for especially government organisations.

8.2.2 All Information Technology equipment and software acquired by the Municipality must be used by and for Tswelopele Local Municipality and the mandate that the

municipality has in accordance with the laws of the country. The use of these assets must benefit not only the municipality but also the community that the municipality is instructed by law to attend to and oversee. The length of the usage should not be less than three (3) years. A common Information Technology solution should last between three (3) and five (5) years provided there is no dramatic change in technology.

8.2.3 The equipment and software should be used responsibly and within the manufacturers specifications and in no way be abused for personal gain, roughly handled to such an extent that the equipment may be damaged or use to further an organisation other than the government and municipality.

8.2.4 Components of the computer hardware may not be removed from the computers unless the computer fails due to normal usage or an act of God such as lightning or floods that renders the computer as a whole unusable but components there-of still usable. Such components should be allocated to government computers only and should be installed to improve such equipment where improvements are necessary and may not be sold or given to private individuals or organisations.
This may include RAM chips, hard disks, processors (CPU's) and cables and even VGA adapters (screen cards).

8.3 MANAGEMENT OF ASSETS AND RECORDKEEPING

8.3.1 All Information Technology assets must be listed in a register or inventory in either manual or electronic format and should be updated regularly. This inventory must be verified and spot checks on equipment should be done along with regular services.
Because of the nature of Information Technology equipment and software it is very important to maintain strict control over it as abuse and theft can easily be committed.
Software can be used on many computers without traces of such theft until checks are done. Using software illegally can result in all parties involved being charged with software piracy and theft and the onus is then on them to proof otherwise. Hardware components can show up

easily as being stolen by checking system configurations against what was issued to personnel or installed on their computers. Common items stolen are RAM, cables and hard disks. In some cases processors (CPU's) have been stolen and replaced with one of a lower performance level.

8.3.2 A network and computer management program should be installed to keep track of computer and file server hardware configurations and indicate where changes have occurred on computers and file servers. It is not uncommon for such items to be stolen or taken and replaced by lesser components. Such programs are available to audit such equipment and report any changes according to the compiled configuration inventory for a computer or file server.

8.3.3 Regular audits should be carried out on computer equipment to control and manage Information Technology assets. Reports should be made out to the Office of The Director of Corporate Service responsible for Information Technology and the report must then be tabled to the Executive Committee to provide feedback. It should also serve as information on the management and control over assets within the municipality and govern any action against people guilty of contravening control and management policies and instructions over assets.

8.3.4 As with cars computers do have moving parts and these parts are negatively affected by dust and smoke particles in the air. The equipment must be serviced at least every three (3) to six (6) months to clear away especially dust and to ensure that the components are not covered by dust which results in heat building up.

8.3.5 No person should smoke in the server room at all. No food or drink should be allowed in the server room as spillage may damage the equipment. It is also advisable and recommended that no person may smoke near computers as to ensure better protection and also better performance and longer life from the equipment. Since smoke can build up to dust it is prone to form a layer like dust and cause failure in sophisticated chips. Failure through heat build-up is common with computer equipment.

8.3.6 The movement of computer equipment must be done with a project plan as this movement usually affects other areas such as IP Addresses and network segments but especially hub population and configuration. In extreme cases such changes also meant a change in router configuration. Such a plan must reach the Office of the Director of

Corporate Service responsible for Information Technology no later than at least thirty days in advance to ensure proper planning and to properly inform users of such movements and how they will be affected.

9. PATCHMANAGEMENT POLICY

9.1 PURPOSE OF THE POLICY

The purpose of this policy is to ensure that all computers and servers are patched correctly by implementing steps that are precautionary and not remedial.

9.2 PRIORITIZINGWINDOWS DESKTOP PATCHES

This list covers the major categories of things that can be patched or updated in a typical desktop configuration and the order in which you should apply them whenever possible.

1. **Bios:** As with servers, start here. Managing BIOS updates across multiple systems is all the easier when they're of the same make and manufacturer, but it requires "hard" downtime: The computer has to be powered down and rebooted to apply the new BIOS, and the administrator usually has to baby-sit
each system individually that will be upgraded. Fortunately, many PC manufacturers now allow centralized updates to BIOSes through a management application -- Altiris, for instance, has a management solution for Dell desktops and notebooks that allows remote BIOS updates.

2. **Device BIOSes:** These include things like BIOS updates for disk controllers, video cards or other devices. Device BIOS updates go into a separate category from regular BIOS updates for two reasons: One, they are easy to overlook and not often considered for desktops; two, you usually cannot update them en masse. For example: If you're administering a group of graphical workstations that need updates to their video card's BIOSes -- and the only way to do that is via a 16-bit DOS-based updater -- you'll probably have to do that by hand for each computer. However, if you could perform the update through a 32-bit Windows application, you could probably push out your Windows patches as you would any other update.

3. **Device drivers:** As with servers, one of the more common hardware device driver updates published for a desktop computer is for the network controller. Make sure you test the update ahead of time. If you automate patching on a whole slew of machines with such a driver and the end result is that they're all knocked off the network, your only choice might be to either re-image them from scratch or fix each one manually.

4. **The OS:** Patching Windows OSes is the part almost everyone is directly familiar with and it needs relatively little elaboration here. One thing I'll add is something I also wrote about in the server version of this article: If there are device driver updates, they should be examined separately from other updates in case an OEM-provided version of the driver is more urgently needed.

5. **Middleware:** This normally includes elements such as ODBC drivers but should also include things like the Microsoft .NET Framework. Note that with the .NET Framework, the 1.1 and 2.0 iterations (and the upcoming 3.0 edition as well) exist side-by-side and don't eclipse each other.

6. **Application patches:** As with the OS and its attendant patches, you can roll out application patches through the usual automated mechanisms, and it should be done only after everything else has already been applied.

9.3 MANAGING YOUR PATCH TESTING BUDGET

The biggest Windows patch management costs related to creating a test lab are hardware and software. Although both are necessities, there are some ways that you can really hold down the costs. Let's talk about the hardware first.
One way you can economize on hardware is to purchase PCs instead of servers. If all you do is test the impact of occasional patches, then you don't need things like multiple processors and RAID arrays.
You can save an absolute fortune just by using a basic PC with plenty of disk space and memory for testing purposes. Another cost-saving technique is to use **virtual machines**. Products such as Microsoft's Virtual Server 2005 and VMware from VMware Inc. allow you to simultaneously run multiple virtual computers on a single physical computer.

9.4 REDUCE COST OF MICROSOFT PATCHMANAGEMENT SOFTWARE

Try using Windows patch evaluation software in your lab. Microsoft offers 120-day evaluation copies of most of their products for free. Therefore, if you are testing an entire patch management configuration, a single patch, an upgrade or whatever for less than 120 days, you could just download some evaluation software and not have to worry about the cost.

9.5 USING THIRD-PARTY PATCHES

Most of us have been there before. It's the beginning of the month, Patch Tuesday is about ten days away and we hear about a new exploit that we know we are susceptible to. At such a time, it's frustrating to know we have to wait for the second Tuesday of the month before a software fix arrives. You might think that deploying a third party patch is a good idea. Well, sometimes it is. And sometimes it isn't.

9.6 THE CONS OF THIRD-PARTY PATCHES

IT administrators deploying off-cycle patches from third parties, in many instances, will have no idea what the patch contains. So before you consider deploying an off-cycle patch, you should ask yourself how much you trust the company that produced it. Even patches from a company without any malicious intent can inadvertently be infected by malicious code. In the worst case, if a company producing third-party patches has less than honorable intentions, it potentially could distribute a patch containing spyware or code that makes it easier to exploit the vulnerability that the patch supposedly addresses.

Another potential problem with deploying third-party patches is that these patches might break parts of your system that are currently running just fine. After all, in the case of a Windows patch at least, many of these fixes are actually replacing operating system code. Even the slightest change to code could have catastrophic effects.

9.7 THE PROS OF THIRD-PARTY PATCHES

In the opinion of some Windows security experts, the risk of accidentally introducing bugs or malicious code into a system, along with the risk of Microsoft not supporting the system, far outweighs the risk of having to wait for a legitimate Microsoft patch. After all, Microsoft does have a history of expediting patches for more serious security issues. At times, Microsoft even provides detailed instructions on how to protect a system against a newly discovered vulnerability until a patch can be produced.

Essentially then, the debate between using third-party patches and waiting for Microsoft patches comes down to an issue of timing. If you feel you are facing a serious Windows security vulnerability and Patch Tuesday is weeks away, you might want to run the risk that the third-party patch could produce bugs just to protect yourself from greater danger. If the risk is not so great, you might want to just wait for Microsoft to release their own patches.

9.8 WINDOWS PATCHMAINTENANCE AND POST-PATCH SECURITY

Be mindful of changes in general system behaviour.
If something is clearly wrong, it'll tend to announce itself. That said, this is a little easier to do when you are solely responsible for the system in question -- for instance, a server.
If you deal with multiple workstations, stay close to one of the patched machines, if you can, and if anyone reports bizarre behaviors, you can investigate them and then try and duplicate them on your own "pet" machine.

Inspect the system logs.
Compare error logs both before and after a patch, and see if anything new or unusual jumps out at you. Sometimes it might not be anything, or it might be coincidental, but error logs are one of the best places to go to for concrete information about something not working correctly. This is especially important if what is going wrong has no other outward symptoms yet, except for a logged error. (Also keep in mind that some errors may simply be false alarms and have no real connection to anything; sometimes it can be hard to tell the difference.)

Check compatibility on any potentially affected applications.

If there's a chance a given patch might affect the way a program works, test it before and after the fact. For instance, test a patch to a middleware component by making sure no database connections are suddenly throwing errors. In addition, make sure other non-trivial database operations that take place in your environment -- and that require middleware (like retrieving large amounts of data or opening many connections at once -- also get tested whenever possible.

9.9 ROLLING BACKWINDOWS PATCHES

Roll back by hand

Microsoft's hotfixes and service packs for Windows come pre-equipped with their own Windows patch rollback mechanisms that can be activated manually if the need arises. If you want to uninstall a given hotfix, here's the procedure for doing so.

1. Set Explorer to show hidden and system files if you haven't already done so.

2. Open the**%SystemRoot%** directory and look for a series of directories with the name **$NTUninstallKBXXXXXX$**, where XXXXXX is the Knowledge Base article number for the hotfix in question.

3. Within that directory is another directory named **spuninst**.

4. Inside **spuninst** is an executable named **spuninst.exe**. Run it, and the hotfix in question will be rolled back through a Wizard interface.

5. If **spuninst.exe** doesn't work or is unavailable, type **batch spuninst.txt**. This executes a batch-file version of the sam recovery options.

System restore

Windows also has a global mechanism for restoring settings and components to an earlier state. It's one most of us should be familiar with: System Restore. This method is something of a brute force way to move back to before a hotfix was installed. And it's slow -- it can take many minutes for a System Restore to complete -- *but* it covers absolutely everything that might have been touched by a hotfix.
Be mindful, though. You cannot run System Restore from the Recovery Console, at least not without a good deal of manual hacking. However, you can run an individual patch rollback as described before from the Recovery Console.

Third-party software

The most complete way of dealing with patch roll back is probably through a third-party package. Plenty of third-party software products exist for rolling a system back to an earlier state, with undoing changes made by patches as part of that.

9.10 FIXING POST-PATCH PROBLEMS: AUDITING REVISION LEVELS

Just because you patch something once doesn't mean that you won't have to patch it (or something else) later. The list below details how you can audit revision levels to fix problems after deploying Windows patches.

In Explorer:

The most obvious way to determine the revision of a component is just to right-click on it in Explorer and select Properties | Version. Or, you could switch to the Details view in Explorer and show the File Version and Product Version as columns. But, with this view, you can't easily export the results. Note that .DLLs will have a Version tab, but .EXE files will not, so this limits its usefulness a bit.

Through Process Explorer:

The endlessly useful Process Explorer utility from Sysinternals lists the revision levels of all loaded components. If you click on the name of a process and select View | Lower Panel View | Show DLLs, you can see all of the loaded DLLs in use by that process as well as their revision levels. This is only useful for running processes, but the program does support exporting the information shown to a delimited text file. Note that it may take several seconds for the program to poll all the used .DLLs for a given process.

Through an external resource:

This method is best if you want to find out what other revisions there might be for a process or component. For Microsoft components, Microsoft itself has a site called DLL Help. There you can look up any component from a Microsoft or Microsoft-supported product, see all of the tracked revisions for the component and learn more about each of them. However, DLL Help is only useful for Microsoft components, not third-party apps.

Through a script:

This option is the most effective way to report back on a whole slew of components at once. For instance, use a script if you want to audit all of the items in a directory that represent what a patch will put into place, and you want to see a quick side-by-side comparison of component revision information. One such script is available online at JSWare and, with a little work, it can be used to obtain the revision information for all files that match a wildcard or are in a directory.

9.11 DOWNLOAD FILESWHEN AVAILABLE

One of the first things that is recommended in Windows patch management is configuring Windows Server Update Services (WSUS) to download patches as soon as they are available, not when they are approved. Normally, patches are not downloaded until you approve them. The problem with that is that as soon as patches are approved, computers try to install them. If the patch has not yet been downloaded though, the update process has to stop and wait for the patch to be downloaded. This whole process can be made more efficient by downloading files as soon as they become available.

To change the download option:

- Open the WSUS Admin console and click the **Options** button in the upper left corner of the screen.
- When the **Options** screen appears, click the **Synchronization Options** link
- Scroll all the way to the bottom of the screen and click the **Advanced** button.
- The **Advanced Synchronization Options** dialog box will appear.
- Make sure that the **Store Update Files Locally** option is enabled and that the **Download Update Files to This Server Only When Updates Are Approved** option is not selected.

10. FIREWALL POLICY

10.1 PURPOSE OF THE POLICY

The purpose of this policy is to ensure the protection of all computers and data on the network by implementing steps that are precautionary and not remedial.
This includes computers making outside connections through secure channels and not through the file server.

10.2 PROFILE SETTINGS

You can use these policy settings to configure Windows Firewall for each kind of network profile.

TURN ONWINDOWS FIREWALL

DOMAIN PROFILE

On computers to which this policy is deployed, this policy setting controls Windows Firewall while the computers are connected to domain networks, such as at a workplace.

- **Yes** enables Windows Firewall on managed computers while they are connected to domain networks.
- **No** disables Windows Firewall on managed computers while they are connected to domain networks.

Recommended value: **Yes**

PRIVATE PROFILE

On computers to which this policy is deployed, this policy setting controls Windows Firewall while the computers are connected to trusted networks, such as a home network.

- **Yes** enables Windows Firewall on managed computers while they are connected to trusted networks.
- **No** disables Windows Firewall on managed computers while they are connected to trusted networks.

Recommended value: **Yes**

PUBLIC PROFILE

On computers to which this policy is deployed, this policy setting controls Windows Firewall while the computers are connected to untrusted networks at public places, such as at airports or coffee shops.

- **Yes** enables Windows Firewall on managed computers while they are connected to untrusted networks.

- **No** disables Windows Firewall on managed computers while they are connected to untrusted networks.

Recommended value: **Yes**

11. CONCLUSION

The network and Information Technology as a whole is very important to any organisation and abuse of such services may lead to large bills in support and repairs as well as security breaches in some cases. Unfortunately strict action is important and cannot be ignored and users should be made aware of such actions. There cannot be a scenario where freedom reigns on the network and users have free access to do as they please.

It is very important to control and properly implement the policy to act as a tool to ensure such control and to ensure that the relevant performance and security levels are reached on the network and with Information Technology as a whole.

The policy on ensures the protection of the government employee and the interests of the government, locally, provincially and nationally. Without such control measures the transparency policy is not adhered to and a secure network becomes insecure, unstable and very expensive to maintain.

12. REFERENCES

- Microsoft Windows 2003 Server administrators Pocket Consultant 2nd Edition (William R. Stanek) ISBN 0-7356-2245-6

- Microsoft Windows Security Resource Kit 2nd Edition(Brian Komar) ISBN 0-7356-2174-8

- Microsoft Internet Security & Acceleration Server 2004(Bud Ratliff & Jason Ballard) ISBN 0-7356-2188-8

- www. computer-policy.com

- www. attackprevention.com

13. ACCEPTANCE OF POLICY

All employees that are granted the use of I.T. equipment will be provided with a written copy of this policy.

Employees must sign the statement below as acceptance of this policy.

I, _____ ID. No. _____

(Full name printed)

Employee No. _____ hereby accepts the terms and conditions of Tswelopele Local Municipality's Information Technology Security Policy. I understand that disciplinary action will be instituted against me should I breach any clause of the said policy.

Signed at Tswelopele Local Municipality on this _____ day of _____20_____.

_____

Signature

As witnesses: 1._____

2._____