

# S O L G M

NZ SOCIETY OF LOCAL GOVERNMENT MANAGERS



## MANAGING THE ELECTRONIC INFORMATION

### Appendix A Part 14

Code of Good Practice  
For the Management of Local Authority  
Elections and Polls

Produced by the  
SOLGM Electoral Working Party

# Contents

|   |    |
|---|----|
| Introduction . . . . .                          | 3  |
| Objective . . . . .                             | 3  |
| Legislative requirements . . . . .              | 3  |
| Recommended practices . . . . .                 | 4  |
| Physical security . . . . .                     | 4  |
| Network security . . . . .                      | 5  |
| Data security . . . . .                         | 7  |
| Staff organisation . . . . .                    | 8  |
| Communications security . . . . .               | 9  |
| Data interchange . . . . .                      | 9  |
| Computer operating systems . . . . .            | 10 |
| System performance factors . . . . .            | 10 |
| Application software . . . . .                  | 10 |
| Results reporting . . . . .                     | 12 |
| STV calculators . . . . .                       | 12 |
| Barcodes on voting documents . . . . .          | 15 |
| The Electoral Roll . . . . .                    | 15 |
| Voting document processing procedures . . . . . | 16 |
| Audit trails . . . . .                          | 18 |
| Miscellaneous . . . . .                         | 18 |
| Glossary . . . . .                              | 20 |
| Finally . . . . .                               | 21 |

# Introduction

Current practice in New Zealand is to use electronic information systems to run local authority elections. Data is captured into a database, verified, corrected and then used to calculate results.

The running of a successful election, when using a computer system, relies on the application of professional standards and processes in all aspects of the election process. Often, those standards are maintained by professional IT personnel.

This section of the Code lists the areas in which IT best practice needs to be applied. Some factors are described in depth, while others are not. In either case, this section of the Code catalogues the factors that the electoral officer needs to be aware of and discuss with their IT professional if they have one.

The Code describes the risks to running a successful election posed by an information system that fails or is compromised by persons within or outside the EO's team.

This section applies equally to elections run under FPP and STV, with the exception that under STV, the result of each election must be calculated using a certified STV calculators provided by the Department of Internal Affairs.

## Information about STV elections

For definitive information about STV elections, refer to Schedule 1 of the Local Electoral Act 2001. Further information can be found from [www.stv.govt.nz](http://www.stv.govt.nz)

## Objective

To make the electoral officers aware of the Information Technology issues and risks to be considered when using a computer network to help run an election. Also, to clarify the procedures dictated by the regulations when using a computer system to electronically record and count votes.

## Legislative requirements

### Local Electoral Act 2001

Section 139 of the Act defines what the regulations may cover. In particular, they cover the use of electoral rolls, generally, and also the prescribing standards, performance measures, procedures, and forms for the conduct of elections or polls. All of the conditions and restrictions involving recording and counting software are found in the regulations.

Where sections of the Act or Regulations have been illustrated, these should be taken as a guide only and are not intended to replace any of the wording of the Act or regulations as published. Nor does any interpretation of the Act or Regulations in this Part of the Code necessarily arise from a legal opinion.

# Local Electoral Regulations 2001

Key regulations affecting the use of a computer system are:

## For FPP elections

|               |  |
|---------------|--|
| Regulation 31 | Order of candidates names on voting documents    |
| Regulation 56 | Processing voting documents during voting period |
| Regulation 57 | Processing voting documents after voting period  |
| Regulation 58 | Counting votes                                   |
| Regulation 59 | Checking systems                                 |
| Regulation 60 | Performance standard for checking systems        |

## For STV elections

|                 |  |
|-----------------|--|
| Regulation 91   | Interpretation                                   |
| Regulation 101  | Processing voting documents during voting period |
| Regulation 102  | Processing voting documents after voting period  |
| Regulation 103  | Counting votes                                   |
| Regulation 104  | Checking systems                                 |
| Regulation 104A | Performance standard for checking systems        |

## Recommended practices

### Physical security

#### Server

If the server is not located at the election office, find out where it is located and ensure that physical access to it is restricted and secure. Find out who has authorised access. These persons will need to be aware of the election timetable so that the server is not removed from service at critical times.

Maintain a list of authorised users of the server.

Have one main contact person who works in the network team and keep that person informed.

#### Workstations

The workstations (PCs) need to be located in an area accessible by only authorised persons at all times.

#### Backups

Ensure that backups that are taken regularly from the database are stored safely and securely offsite away from the server itself so that the server and its backups cannot be damaged or destroyed simultaneously.

Maintain a backup log.

A fire-proof safe should be used for storage of backup media with security access being carefully controlled.

Offsite storage companies can be employed with transportation of media being via a secure courier. One-hour return should be available.

Backups should be securely erased or destroyed after the election. Backup tapes should be destroyed, not simply discarded or reused. Backups made to a hard disk system are not fully erased until the data is overwritten with null or other data. Deleting the files is not sufficient. This is especially important when a rented server is returned to the supplier.

## Network security

### Connection to the Internet

Your very best strategy is not to have your election computer network connected to the Internet or to any other corporate network. If you have a choice, this is the safest approach from a security point of view. In particular, there should be no wireless access to the election network

Should you need access to email or to the Internet, you can get this through an alternative PC connected to your corporate network.

If you need to connect your election network to a wider corporate network, you should specify to your IT service provider, what software applications you wish to enable on each of your networked PCs. The email server, web proxy server and firewall can be configured to allow or disallow any services that you need, without compromising your security

### Software currency

Ensure that the firewall, proxy server, email server and all other network components are completely up-to-date with security patches.

Ensure that the firewall, proxy server, email server and other devices on the network provide completely up-to-date virus protection.

Ask your IT service provider about software to detect, alert, and prevent an attack to or through the firewall.

### Virus protection

Ensure that every PC in the election network is protected with an up-to-date anti-virus system.

Prevent software or documents of any sort being downloaded from the Internet or from a disc, iPod or similar device. Have all your networked PCs, other than an administration machine, configured so that diskettes or portable storage devices of any sort cannot be used to copy files onto them. One centralised resource drive is the best way to contain the upload of unauthorised software.

### Server access

Ensure that only authorised IT administrators can log onto the server. You may wish to have those persons sign the declaration that other election staff are required to sign.

Ensure that only nominated persons can make a logical connection to the server share that contains the database.

## Network recovery

Ensure that there is a plan in place to recover from a failure in any component of the network which has the potential to stop the processing of returned voting documents. Determine the availability of spare network components.

You may need to upgrade the network infrastructure in the election office, providing additional ports for the computers, printers and other equipment. Before this can be done, you will need a plan of the proposed layout for all your PCs, printers and other network equipment. An as-built diagram of the network will be required by an engineer to assist in identifying problems.

## Single Image on network PCs

The personal computers being used in the counting process should ideally all be of the same specification and share the same configuration image, operating system and hardware profile. An image should be built and tested, then copied onto multiple machines using such software as Norton Ghost or similar. This image may be pre-loaded by a hardware rental company or by in-house technicians. The image should again be tested in a networked environment prior to Election Day. Keeping each PC identical may save you time in maintenance or fault-finding.

A backup copy of the image should be retained in the event that a re-count is required or in case the image is required as part of a scrutineering process.

## Wireless networks

Wireless networks, if employed, can introduce additional security risks and should be implemented with caution, and avoided if possible. WPA security (or better) with MAC filtering should be considered a minimum standard. WEP security is not considered secure for this purpose.

## Networked PC usage

Ensure that the PCs have virus protection software installed and enabled at all times and that virus definitions are up to date.

Adopt a rule that no PC operator shall insert a removable diskette or CD-ROM into any PC. Under Windows/2000 or Windows/XP it should be possible to restrict access of CD-ROM drives and diskette drives to the Administrator password only, thus preventing access by other users.

Ensure that the PCs cannot be used to access the Internet, or to access email programs. Ensure access by portable storage devices is prevented (such devices for example that plug directly into USB ports).

## PC start-up and operation

Ensure that PC's are configured so that the start-up sequence does not allow booting (start-up) from a floppy disk, CD ROM or external media device accessed via USB or other port that may effectively compromise security.

Ensure that all PCs will automatically become locked after a few minutes without use. This is normally accomplished through the "screen saver".

Ensure all your election network users understand the rules you have established for the use of the network. If Internet access is possible from the users' PCs (which is not recommended) let them know that such usage is monitored to their PC and to their Username and ensure that this is undertaken periodically.

## Username and passwords

Username and passwords for data entry operators should have been created so that the initial passwords expire at the first login for each username. Users must then choose their own private passwords.

Generic or systematic usernames (e.g. "User1") can too easily be guessed and therefore should never be used on a continuing basis.

All usernames that are not required or are no longer to be used should be removed immediately.

Passwords should conform to the council's password policies, and should meet the criteria for strong passwords (6 characters or more in length, contain a combination of letters, numbers and special characters, and not be easily guessable).

## Screen-saver locks

Ensure that all PC's are configured for the screen-saver lock to activate when the PC is not used for more than 5 minutes. This will help users who may not be good at locking their PC whilst unattended. Remind your users to lock their PC - this is largely a cultural issue, make it a team priority.

## Data security

### Backup schedule

Discuss with your IT person when the election database will be subject to incremental and full backups.

Ensure that the backup plan never results in you being without a recent full backup of your database, even if only for a very short time. Never make a backup that overwrites your previous best backup.

Ensure that you have a full backup of the fully configured system before beginning the vote counting.

### Document retention policy

Create a document retention plan. This is to ensure that all electronic documents or data on which the conduct of the election depends or which document the progress of the elections, are included in the backup schedule at least once per day.

Include important emails in the document retention plan.

### Recovery plan and testing

Determine, in advance, how long it will take to restore the database from backups onto the same or a replacement server.

Make sure that the backup and restore process is fully tested with realistic data before voting document processing begins.

After voting document processing begins, have the IT staff restore a backup onto a test machine, and check that the data is correct.

Ensure that the server database is configured for transaction logging so that, in the event of a server failure or database corruption, data loss is minimal.

Discuss with your IT staff, how you will determine what data is in the database after recovery from a failure.

Ensure that you have adequate replacement hardware for all components of the system in case you should lose one or more components during voting document processing. Ensure that support agreements detail the response time and recovery or break-fix time and that these timeframes are appropriate.

## Staff organisation

### Staff checks

Ensure employees are police-checked and check references that you may have required. Where else do your employees work, are there any conflicts of interest? Data losses are often deliberate as opposed to accidental. You need to understand the triggers that cause people to act other than in your best interests.

### Separation of duties

Where possible, staff duties should be separated to ensure that any person's work is checked by a different person.

The separation of duties must be supported by application software through the use of a unique logon username for each person.

### Acceptance of responsibility

You will already have a non-disclosure agreement for all staff to sign relating to security of election data and processes. Extend the agreement to include destruction, damage, or attempt to invalidate any software or hardware in use for the election process. Have all staff sign this, including those with administration rights over the server and network.

### Staff training

Before the early processing period begins, you should ensure that all your staff, who are unfamiliar with the software that you are using, are trained to use it. This may require the creation of an instructional booklet if a software user's guide doesn't already exist. The guide should describe clearly and simply how to deal with the most commonly expected problems.

It is strongly recommended that you establish a training environment on your network and allow your staff to practice using it before they are required to use the production system.

### PC usage

Emphasise to all staff that they must...

- Logout of their PC before leaving it unattended.
- Never share their login password with anyone else.
- Not let another person use their PC unless first logging out.

## Building access

Ensure those staff employed for processing of election results have sufficient security access to the building during the period of election processing.

Where security cards are in use, ensure these are tested prior to the day/s of operation.

## Communications security

### Email

Access to email should be carefully controlled to prevent unauthorised communication of results.

Only a single secure PC, secured to the EO's password, should have email available for communication of results to outside parties.

### Internet

Where results are to be communicated via the Internet, sufficient preparation and testing of processes must have been undertaken to ensure results can be successfully presented.

Presentation of election results over the Internet could be thwarted by denial of service (DoS) attacks on the Internet server. Contingency plans are required.

The Internet server should be adequately protected with firewall and anti virus protection, and preferably intrusion-detection software

### Printing

Access to unauthorised printer hardware outside of the electoral office should be restricted.

## Data interchange

When any data is exchanged between computer systems operated by different organisations, (for example, data captured locally and forwarded for central processing in a DHB STV election at large), a copy should be kept of any data sent to another site, both as evidence of what was sent, and in case the consignment is lost.

At the time of writing, there is no national standard for such data interchange. The format used are the result of mutual agreement between all parties concerned.

Any data that is transferred electronically (e.g. by email or an attachment) should be followed by the data also sent on a medium such as CDROM, because electronic exchange of data may not be adequately covered by an EO's insurance policy.

Any media sent to another site should be signed and dated by the EO or his representative. The EO should also label any retained copy in the same way as the original.

Any media used for such data exchange should, if possible, be such that the data written onto it can not be altered in any way without such alteration being clearly evident. Discuss this issue with other parties with whom you plan to exchange data. A simple, but very effective approach is to use the SH1 secure hashing process. This enables you to generate a reliable electronic signature for each data file and transmit the signature with the file.

If you are concerned about other parties intercepting and using the data you are sending, use encryption. Encrypt the data you wish to protect prior to any data interchange. Use a reliable encryption method such as Public Key Encryption. No Encryption method is entirely secure but the time taken to decrypt good methods extends beyond the useful life of the data

## Computer operating systems

### Security updates

Ensure that the PCs and the database server are running with operating systems updated to the latest available patch level.

### Compatibility

The PCs must be running an operating system compatible with the application software and the STV calculator (for an STV election) The two certified DIA<sup>1</sup> STV calculators require Windows 2000 or Windows XP.

## System performance factors

### Performance testing

Ensure that the database server provides an adequate response time with the maximum number of network PCs doing data entry simultaneously. Make sure that the software provider has done adequate testing for your particular situation. Otherwise, organise a full-load test yourself.

### Server data capacity

Obtain a reasonably accurate estimate of the maximum size of your database.

Ensure that the server can accommodate your database with an adequate additional capacity. Ensure that the server provider has allowed an adequate margin for the database transaction log.

## Application software

### Software certification

In an STV election, you must use one of the STV calculators provided by the Department of Internal Affairs. Both calculators have been certified by an approved certifier.

Ensure that the application software package that you use for the election is also certified by a reliable certifier. If you need to, consult the DIA before signing a licence agreement. Preferably, the software (even though in an earlier version) should have been used in a previous election. Make sure that the version you are planning to use has been certified. You should ask for copies of the certificates and check them against the version numbers built into the application software.

If you receive a new version of the application software, it needs to be accompanied by an updated certificate and documentation that describes the changes made since the previous

---

<sup>1</sup> There may be, although unlikely, other certified STV calculators.

version that you have used or tested. Make sure you read the documentation and are very clear about the changes that have been made.

If you wish to test the modified software, do this first in a test or training environment.

### Supplier support

Discuss with your application software supplier, the action that the supplier will take if the software fails for any reason. Have the supplier provide phone numbers for you to contact them during and after office hours, and especially around the close of voting.

### Access to reporting tools

Ensure that the software components to be used to calculate and report election results are installed on only those PCs that are to be used for reporting, and that the software can be run only by persons that are approved to do so. For further security, you can delay the installation of the reporting tools until just before they are required to be used, provided that the installation process has been previously tested.

If you are using application software that contains time and password locks on the reporting tools, this should not remove the need to take further restrictive measures such as those above. Paranoia is OK!

### Access to intermediate files

Where intermediate files are used to link the data collection and the calculating/reporting parts of the application software, ensure that those files are held on a secure server with access limited by authorised people only.

### Locking by passwords/password safety

If any part of the application software (such as the reporting tools) is to be locked using one or more passwords, ensure that the administrator password has been documented correctly, is stored in a physically secure location with restricted access and is obtainable in an emergency.

The use of password controlled locks on counting software is not prescribed by the regulations or the Act. It is a mechanism used in some election software to restrict access to the trends of an election while voting is in progress. Ultimately, it is the responsibility of each EO and of all persons involved in early processing of voting documents to ensure that voting patterns are unable to be determined. Therefore, software locks should be used if they are provided by the software.

User level passwords should not be recorded anywhere, as these can be reset by the Administrator account if necessary (and this should be auditable). The Administrator account should not have access to election data.

### Data security

Persons with IT responsibility, who are assisting the EO, must take whatever steps they can to protect the recorded votes from being inspected or counted before close of voting.

On the other hand, the EO may require some assurance that votes are indeed being recorded into the database, and there is not an undetected gross malfunction of the software. The EO's IT staff may be required to generate some progressive summary statistics from the database to match against the number of voting documents known to have been processed.

## Software automation

It should be possible under Windows/2000 and Windows/XP to control access to certain software applications only, with the possibility of the vote entry software being automatically started on sign-on, and sign-off being automatic on exiting this software.

Removing the ability to run other applications concurrently on the data entry PCs also reduces the chance of conflict between processes that may corrupt the vote entry process.

## Results reporting

*The Local Electoral Regulations were amended in December 2003 and now allow the electoral officer to announce the preliminary results of the election. Regulation 61A relates to preliminary results for FPP elections and Regulation 105A relates to preliminary results for STV elections.*

### Electronic document types

Decide in advance the document types with which you will report the results and inform all the interested parties of this.

If you plan to distribute results electronically, inform the recipients of the name and version numbers of the software they will need to read your distributed documents.

Preparation of email distribution templates

At an early stage, gather lists of persons to whom you wish to send results. Build the email addresses into email templates along with the covering descriptive text. Save the templates for use after close of voting. Make sure that you test all email addresses well in advance of needing to use them.

### Manual editing of results

Try to avoid having to manually edit results documents before they are distributed. If this is not possible, keep copies of all the documents before editing and at any other intermediate stages of the editing process, so that the manual process can be easily audited afterwards.

### Printer hardware

Printing hardware should have been pre-installed and tested on the network where result printing is to be performed.

## STV calculators

### Prior testing of the main and backup STV calculators

Ensure that the process for using BOTH the main and backup calculators is determined and documented for your situation. Have both calculators installed and ready to use after the data capture is finished. In the unlikely event of you having to use the backup calculator, make sure it can be used without delay.

*You should refer to the DIA's web site [www.stv.govt.nz](http://www.stv.govt.nz) to find the latest recommended procedures for the use of the STV calculator.*

## Support for the STV calculators

Details of how to obtain support for the main and backup calculators will appear on the STV web site [www.stv.govt.nz](http://www.stv.govt.nz)

## Timetable for results calculations

Work out a plan for calculating the STV issues in the required order. Use the supplied test data to obtain an estimate, on your own hardware, of the likely time to calculate each issue. If you need to, plan for running a number of STV calculators simultaneously on a number of suitably configured workstations (PCs). Have a detailed plan for loading the required data into each separate PC that will run the STV calculator. Thoroughly test the whole process with your own report templates and the best test data you have available.

## Access to the STV calculator

Ensure that only a selected number of people can run the STV calculator.

Ensure that the STV calculator is installed to run on the selected PCs in the election office and that only approved persons can log onto those PCs.

## Minimum requirements to run the 'main' calculator

The following definition is from the document "STV Installation Guide v0.3.doc" from CGNZ Ltd, who supply the main calculator.

"This section outlines the minimum requirements for the STV calculator operating platform. These requirements should be met to ensure the STV calculator functions correctly and efficiently. The minimum requirements are hardware and software dependent, and are outlined below.

### Hardware

- Intel Architecture Pentium 4 or equivalent
- 512 MB Ram
- 100 MB disk space

### Software

Either one of these operating systems can be used.

- Microsoft Windows 2000 Professional – Server Service Pack 3
- Microsoft Windows XP Professional – Service Pack 1

## STV calculator comparisons

There are significant differences in the performance and the installation requirements of the two certified STV calculators.

### Backup calculator

- Requires a SQL Server database to store data and calculate results.
- Is much slower at loading data and calculating results than the main calculator
- If this calculator is used, several calculators on different PCs may be required to calculate a preliminary result at close of voting.

### Main calculator

- Doesn't require its own SQL Server database; all data is held in the PC's RAM.
- Much faster than the backup calculator.

- Most local elections can be calculated on a single fast PC within a reasonable timeframe after close of voting.

While the main calculator is impressively fast and only one PC may be needed to calculate STV results, it would be prudent to have more than one PC available for this task at close of voting.

### Organisation for intermediate files

The STV calculator has been designed to derive the name of its XML-encoded output file from the name of its input file, and to create the output file in the same file-system folder as the input file.

Good practice requires that there be created, in the server's disk filing system, an organisation of folders that clearly separates the intermediate XML-encoded files that contain preliminary and final result data.

The logical organisation of folders will partly depend upon the personal preference of the EO, provided that the organisation chosen helps reduce to a minimum the chance of a wrong file being selected by an operator.

Where an operator is required by the software to choose the name of an intermediate file, there needs to be rules to assist the operator to compose each filename. In particular, filenames should indicate:

- whether the file contains data or results that are preliminary or final;
- the date and time that the data was extracted from the recording database.

### Use of the backup STV calculator

The backup STV calculator is intended for use only when the main calculator cannot produce a result. If a problem arises, you should follow this very brief preliminary check-list.

- **Problem with other software**  
The STV calculator counts votes only when it receives the data input file. Any problems before that point do not involve the calculator.
- **STV calculator does not start**  
Check that the calculator has received the data input file. The calculator cannot start the count until it receives the input file.
- **STV calculator produces error message**  
Analyse message and take appropriate action as per documentation.
- **Problem not resolved and calculator does not produce result.**

Use backup STV calculator.

It is important to note that the two calculators have different requirements. The backup calculator does not include some of the features that make the main calculator easy to use. It is not expected that any electoral officers will need to use the backup calculator.

DIA recommends that the backup (IPL Ltd) calculator is installed on a separate computer to the main (CGNZ Ltd) calculator.

## Barcodes on voting documents

### Use of check characters

When printed barcodes are used on voting documents, the barcodes should contain check characters to reduce the likelihood of data input errors.

## The Electoral Roll

### Roll versions

Leading up to an election, three versions of the electoral roll are normally supplied to an EO by the Electoral Enrolment Centre (EEC). The first is for software testing, the second is the "Checkit" or preliminary roll and the third is the final roll.

Make sure that the printed rolls are produced from the correct database versions, and that the voting documents are produced from the final roll data. The EO must have a simple procedure for knowing which version of the electoral roll is loaded into the database at any stage.

Each roll is supplied with an accompanying printout listing the number of electors in each ward, the number of "194" records and the total number of elector records supplied. Taken together with known numbers of merged ratepayer electors, these numbers can be cross-checked against the entries on the printed ward rolls and against the number of entries on each ward extract file from the database that drives the voting documents paper printing process.

Make sure that all media supplied by the Electoral Enrolment Centre is clearly labelled and made safe.

### Use of the electoral roll data

The electoral roll is compiled from data collected for the sole purpose of running elections. The principles contained within the Privacy Act 1993 limit the use of the electronic electoral roll data to the purpose for which it has been collected; that is, to the running of an election.

The Electoral Enrolment Centre, the agency that has collected the data directly from individuals, supplies the electoral roll to local authorities to run their elections and for no other purposes. Electoral officers and their IT staff need to be aware of this and to ensure that the electronic electoral roll is not copied or redistributed to any other person for any other purpose.

### Keeping the Master Roll

Regulations 69(1) and 114((1) require the EO to retain copies of the final or master roll, as used for the scrutiny, until the next triennial election. Furthermore, the roll must be available for inspection by an elector in the same local government area.

It would be wise to keep the electoral roll on the medium originally supplied by the Electoral Enrolment Centre together with the printable electronic files (including ratepayer electors) derived from it, in case the EO wishes to reprint a roll at any time.

It is clearly a legitimate use, under the regulations, of the electoral roll for an electronic copy to be maintained until the following election on the council's computer network and accessible by a simple enquiry program, to assist enquiries from electors.

# Voting document processing procedures

## Definitions

The Regulations use the following terms in respect of FPP and STV elections, particularly where computer systems are used to process the voting documents

| FIRST PAST THE POST (FPP)   | SINGLE TRANSFERABLE VOTE (STV)  |
|---|---|
| <p><b>"Checking system</b> means a system that:</p> <ul style="list-style-type: none"> <li>(a) is designed to ensure that               <ul style="list-style-type: none"> <li>(i) votes recorded from valid voting documents correctly record the intentions of the voters expressed in those voting documents, and</li> <li>(ii) votes are counted correctly, and</li> <li>(iii) results are determined correctly according to the First Past the Post electoral system, and</li> </ul> </li> <li>(b) may include components that               <ul style="list-style-type: none"> <li>(i) identify errors and processes likely to generate errors, including (but not limited to) components that entail the                   <ul style="list-style-type: none"> <li>(A) repetition of operations and the comparison of the results produced without varying the processes used to perform the operation or by using different processes to perform the operation, and</li> <li>(B) use of selection methods, for example, selecting all operations or selecting operations by type or selecting operations carried over a period of time or selecting selection operations by sampling</li> </ul> </li> <li>(ii) correct errors,</li> <li>(ii) modify processes so that they are less likely to generate errors; and</li> </ul> </li> <li>(c) must, if practicable, correct any errors that it identifies."</li> </ul> | <p><b>"Checking system</b> means a system that:</p> <ul style="list-style-type: none"> <li>(a) is designed to ensure that preferences recorded from valid voting documents correctly record the intentions of the voters expressed in those voting documents; and</li> <li>(b) may include components that               <ul style="list-style-type: none"> <li>(i) identify errors and processes likely to generate errors, including (but not limited to) components that entail the                   <ul style="list-style-type: none"> <li>(A) repetition of operations and the comparison of the results produced without varying the processes used to perform the operation or by using different processes to perform the operation; and</li> <li>(B) use of selection methods, for example, selecting all operations or selecting operations by type or selecting operations carried over a period of time or selecting selection operations by sampling:</li> </ul> </li> <li>(ii) correct errors</li> <li>(iii) modify processes so that they are less likely to generate errors; and</li> </ul> </li> <li>(c) must, if practicable, correct any errors that it identifies."</li> </ul> |

|   |   |
|---|---|
| <p>“<b>Operation</b> with respect to a checking system, includes any act for the purposes of regulations 56 to 58, 78 and 79 and any set of such acts, including (but not limited to) a set of acts defined by sampling.”</p>   | <p>“<b>Operation</b> with respect to a checking system includes any act for the purposes of regulations 101, 102 and 123.”</p>  |
| <p>“<b>Process or processing voting documents</b> means to carry out any process that facilitates the efficient counting of votes, and:</p> <p>(a) includes</p> <ul style="list-style-type: none"> <li>(i) opening returned envelopes</li> <li>(ii) extracting voting documents</li> <li>(iii) rejecting blank or informal voting documents</li> <li>(iv) identifying valid voting documents</li> <li>(v) recording votes from valid voting documents and putting them in a form for counting in an automated counting process; but</li> </ul> <p>(b) does not include counting votes.”</p> | <p>“<b>Process or processing voting documents</b> means to carry out any process that facilitates the efficient counting of preferences, and includes:</p> <ul style="list-style-type: none"> <li>(a) opening returned envelopes</li> <li>(b) extracting voting documents</li> <li>(c) rejecting blank or informal voting documents</li> <li>(d) identifying valid voting documents</li> <li>(e) recording votes from valid voting documents and putting them in a form for counting by a certified counting programme.”</li> </ul> |

## Password testing

All passwords should be pre-tested to ensure they are functional on the day required. Where multiple passwords are required to access a system, passwords should be tested to the lowest level of access. The ability to reissue passwords on the day should be available along with the ability to release user profiles that have been locked from successive incorrect login attempts.

## Counting votes

Regulations 58, 79, 103 and 123A require the electoral officer to determine the preliminary result of the election (or poll) as soon as practicable after:

- (a) all ordinary voting documents have been processed; and
- (b) the close of voting.

The determination of the preliminary result:

- (a) must be made using all ordinary votes; and
- (b) may be made by also using special votes from valid special voting documents identified at that time

In addition these regulations also require the electoral officer to determine the official result of the election (or poll) as soon as practicable after:

- (a) all special voting documents have been dealt with under the regulations; and
- (b) the scrutiny of the roll has been completed and disallowed votes dealt with.

This determination must be made using all votes.

## Checking systems

Regulations 59, 79A, 104 and 124 require the electoral officer to apply a checking system to the processing and counting of votes.

Performance standards for checking systems are set out in regulations 60, 79B, 104A and 124A. The checking system must ensure that the results of the counting are at least as accurate as those that would be produced by:

- (a) carrying out the following operations manually
  - (i) rejecting blank voting documents and informal voting documents;
  - (ii) counting votes from valid voting documents; and
- (b) repeating the operations in paragraph (a); and
- (c) resolving any discrepancies.

In determining whether or not the performance standard is met, it is sufficient to make reasonable inferences about the errors that are likely to be generated by the operation of the checking system.

## Audit trails

### Documentation of system and processes

Documentation of the system configuration, security measures and processes should be available for inspection by scrutineers.

### Traceability

As a general rule, any important manual or partially manual steps need to be traceable. This will include such things as entry of data from batches of voting documents. It might also include any manual adjustments (adding specials) or reorganisation of results between the output from the computer system and publishing of results.

If special votes are managed manually in an FPP election, before and after copies of the results documents should be kept so that the process used remains evident.

The entry of batch data into the computer system needs to be manually logged with date, time and operator information on batch recording sheets.

### Checks for completeness

The EO needs to ensure that processes are in place and reports available from the application software to ensure that all voting documents received are fully processed.

## Miscellaneous

### Know your software!

Regulation 91(2) states that any regulation (from the STV part of the regulations) which refers to a determination or any other action of an electoral officer also includes an action taken by an automated process. So, you need to be aware of exactly what your computer software is doing and be responsible for it!

This explicit requirement is not included in the FPP regulations, although, clearly, good practice requires you to understand your software as best you can under all circumstances.

## Building electricity supply

Have an electrician check the adequacy of the mains power to the election office, sufficient to run all the equipment with a suitable margin of reserve. Be aware that if you start-up all the equipment at the same time, you may overload the supply and lose power. You may need to upgrade the power supply to the election office, or provide additional power outlets for the computers, printers and other equipment. Before this can be done, you will need a plan of the proposed layout for all your PCs, printers and other electrical equipment.

## Electrician

Have an electrician on call at all times when you cannot afford to lose mains power.

## Service Level Agreement

Everything that your IT support organisation promises to do for you should be documented and signed off. A council's IT department will be able to offer you their standard SLA, which you should extend as required. Also ensure SLAs and response plans from all main suppliers (such as the election software supplier) are documented.

## Systems engineer

Ensure that there is a Systems Engineer available for the duration of the election, especially when you cannot afford the network to be unavailable for an extended period. Ensure that you have all appropriate methods of contact, e.g. mobile, pager, home number or that the engineer is on site for the required period. Similarly, organise the availability of an engineer who can fix your server and recover your database at short notice. Ensure that the engineer is familiar with your election database and its configuration. Make sure that all relevant installation and configuration parameters and processes are documented in case the database needs to be recreated on a net server at short notice.

## Server and network availability

Request that there are no planned maintenance outages or upgrades on any component of your system, planned for the period of the election. This should include down-time for air-conditioning systems, or after-hours testing of backup power generators that might affect the server or the network.

## Uninterrupted power supply unit

An uninterrupted power supply unit (UPS) may be worth installing to protect all or part of your system from power fluctuations and also to allow sufficient time for a controlled shutdown should power failure occur. It is particularly important to secure the database server against external disruptions. Ideally back the UPS up with a standby generator to allow continuous operation in the event of a power failure.

## Fire prevention

Adopt a policy of turning off the power to all electrical equipment in the election office during times that the office is not occupied.

## Spare PCs

Decide how many spare PCs and printers you need, and ensure that they are configured ready to use without delay if an equipment failure should occur.

## Provision for judicial recount

When hiring equipment, allow for the possibility that you may need to retain some of the equipment for a judicial recount.

## Data removal

Where any computer has been hired for use in the election, ensure that all software and data has been permanently removed from storage devices before the equipment is returned to the leasing company. Use the US DOD standard 5220.22-M with 7 over-write passes as a minimum standard for secure wiping.

## Workplace safety policy

You must have a workplace safety policy and it must include factors relating to the correct use of computers and the provision of satisfactory conditions for computer operators. There are currently two important documents published by the Occupational Safety and Health Service of the Department of Labour, New Zealand. [www.osh.dol.govt.nz](http://www.osh.dol.govt.nz)

These are:

“Visual Display Unit Safely - How to use your”  
<http://www.osh.dol.govt.nz/order/catalogue/262.shtml>

“Visual Display Units in the Place of Work - Approved Code of Practice for the Safe Use of”  
<http://www.osh.dol.govt.nz/order/catalogue/220.shtml>

Both these documents can be downloaded as PDF files.

# Glossary

## Abbreviations

|      |   |
|------|---|
| EO   | Electoral Officer   |
| IPL  | Information Power Ltd, created the first STV calculator. Now called the “backup” calculator |
| CGNZ | CAP Gemini NZ Ltd, created the second STV calculator. Now called the “main” calculator      |
| EEC  | Electoral Enrolment Centre  |
| IT   | Information Technology  |
| DIA  | Department of Internal Affairs  |
| FPP  | First Past the Post electoral system  |
| STV  | Single Transferable Vote electoral system   |
| USB  | Universal Serial Bus, a type of computer interface connection.                              |
| SLA  | Service Level Agreement   |
| DHB  | District Health Board   |

## Use of the terms 'random' and 'pseudo-random'

Regulation 31(5) defines the terms, pseudo-random order and random order as follows:

- **Pseudo-random order** means an arrangement where:
  - (a) the order of the names of the candidates is determined randomly; and
  - (b) all voting documents use that order.
- **Random order** means an arrangement where the order of the names of the candidates is determined randomly or nearly randomly for each voting document by, for example, the process used to print each voting document.

## Finally

So if, in spite of all this good advice, if your computer network turns to custard and ruins your election, this may help you feel better as you collect your final pay-cheque.

### Why computers sometimes crash!

*If a packet hits a pocket on a socket on a port,  
and the bus is interrupted as a very last resort,  
and the access of the memory makes your floppy disk abort,  
then the socket packet pocket has an error to report.*

*If your cursor finds a menu item followed by a dash,  
and the double-clicking icon puts your window in the trash,  
and your data is corrupted 'cause the index doesn't hash,  
then your situation's hopeless and your system's gonna crash!*

*If the label on the cable on the table at your house,  
says the network is connected to the button on your mouse,  
but your packets want to tunnel to another protocol,  
that's repeatedly rejected by the printer down the hall...*

*And your screen is all distorted by the side-effects of gauss,  
so your icons in the window are as wavy as a souse,  
then you may as well reboot, and go out with a bang,  
'cause as sure as I'm a poet, soon the sucker's going to hang.*

*When the copy on your floppy's getting sloppy in the disk,  
and the macro code instruction's causing uninvited risk,  
then you'll have to flash the memory and you'll want to RAM your ROM,  
and then quickly cut the power, lest it goes off like a bomb!*

Well, that certainly clears things up for me. How about you?

(With apologies to Dr Seuss!)