Elections ACT

Upgrade of eVACS® for the 2020 ACT Legislative Assembly Election

System Specification - Part 1

Requirements

Document Status: Final
Version 1.3
August 2020

Copyright Notice

Disclaimer

In compiling this System Specification – Part 1 Requirements, Software Improvements Pty Ltd has relied upon the accuracy and completeness of information provided by Elections ACT.

eVACS®

eVACS® is a registered Trade Mark of Software Improvements Pty Ltd.

Where used in this System Specification – Part 1 Requirements, eVACS has the same meaning as eVACS®

eVACS® Upgraded Document Tree

- Contract with Upgrade requirements
- Project Management Plan
- Operational Concept Description
- **System Specification - Part 1 eVACS requirements including upgrade requirements**
- System Specification - Part 2 Scenario Analyses
- System Design and Software Specification
- Interface Specification - Setup election
- Interface Specification - Voting
- Interface Specification - IVR - TVS
- Interface Specification - TIGER - TVS & OSEV
- Installation Manual
- User Manual - Election server
- User Manual - Polling Place server
- User Manual - Telephone Voting server
- User Manual - Data Entry

Document Control Information

The controlled version of this document is in electronic form.

All hardcopy versions are uncontrolled.

Modifications

Date of this Revision	Version	Comment	Author	Reviewer	Release
2019-08-05	0.1	Initial Draft	CJB	RB	
2019-09-22	0.2	Split of System Specification into two Parts - Expanded draft of Part 1 Requirements	CJB	RB	
2019-09-27	0.3	Minor edits incorporated together with documentation tree	CJB		
2019-11-27	1.0	Edits after review by EACT and CCP003	CJB		2019-11-27
2019-12-09	1.1	Further edits	CJB		2019-12-30
2020-06-20	1.2	Edits to reflect changed requirements, including menu items & new document tree	CJB		
2020-08-06	1.3	Requirement 89 changed to reflect actual wording of Data Entry Supervisor menu	CJB		2020-08-06

Distribution

Name and Appointment	Document Name	Date of Issue	Version
Jiv Sekhon, eVACS Project Manager, EACT Ro Spence, Deputy Electoral Commissioner, EACT	System Specification Part 1	2019-10-07	0.3
Jiv Sekhon, eVACS Project Manager, EACT Ro Spence, Deputy Electoral Commissioner, EACT	System Specification Part 1	2019-11-27	1.0
Jiv Sekhon, eVACS Project Manager, EACT Ro Spence, Deputy Electoral Commissioner, EACT	System Specification Part 1	2019-12-30	1.1
Jiv Sekhon, eVACS Project Manager, EACT		2020-08-06	1.3

Contents

Lists of Tables & Figures

1. Scope

The System Specification (SSS) specifies the system structure and requirements for eVACS® Upgraded and the methods to be used to ensure each requirement has been met.

The SSS has been derived from the Operational Concept Description (OCD)[3]; in turn it is to be used as the basis for modelling, design, and quality testing of the system.

There are two parts to the SSS:

Part 1 – Requirements, (this document) including election nomenclature definitions as used in eVACS® Upgraded, and

Part 2 - Scenario Analyses, in the form of Event-Action lists reflecting the requirements for the upgraded eVACS®.

Commencing with Part 1 version 1.3 and Part 2 version 1.2, contract change requirements have been incorporated into the SSS.

1.1 Identification

This document applies to the upgraded version of eVACS® to be used by Elections ACT (EACT) in the 2020 ACT Legislative Assembly Election. It is referred to as SSS-1-R.

The purpose of the SSS is to provide the Project Team with a specification of the requirements of eVACS® upgraded. The two parts of the SSS will form the basis for developing a set of Software Requirements Specification (SRS) and Interface Requirements Specification (IRS) documents.

1.2 Document overview

The upgraded eVACS® is based on eVACS® version 7.0 used by EACT in 2016 together with a number of changed or additional requirements to be incorporated for the 2020 Election. The combined requirements are described in Section 3, together with definitions of terms used in association with the requirements. Itemised listings of the definitions and requirements can be found in Tables 1 and 2 respectively.

1.2.1 Definitions, requirements and actions

In section 3, definitions and requirements are interspersed with explanatory text. The content of definitions and requirements is easily identifiable, as each begins with a heading in boldface and includes a unique identifier with the following forms:

Applicable	Identifier	Definition of identifier elements

For definitions:	SSS-D-C-N	SSS = System Specification,
		D = Definition,
		C = Major Section within this document, i.e. 3, and
		N = a sequential number commencing with 1

For requirements	SSS-R-C.X-Y	SSS = System Specification,
		R = Requirement,
		C = Major Section within this document, i.e. 3,

		C.X = a number being a subsection of section 3, where X is a the subsection identifier, and Y = a sequential number, commencing with 1, within C.X

This document is classified as Commercial-in-Confidence.

1.3 Reference Documents

In this SSS-1-R, a citation of the form [1] is a reference to document 1 in the following list.

1. Business Requirements Specification ICT Business system upgrade - eVACS®, version 1.0;
2. Statement of Requirements at Schedule 2 of the Contract Electronic Voting and Counting System (eVACS®) Enhancements, Services and Support: ACTGS reference 636238 Final Version 23 July 2019, being a simplified version of [1];
3. Software Improvements Pty Ltd, eVACS® Operational Concept Description, version 1.1, 2020;
4. The Unicode Consortium. Unicode Home Page available at https://unicode.org/main.html;
5. The Unicode Consortium. The Unicode Standard, Version 12.1 available at http://www.unicode.org/versions/Unicode12.1.0/;
6. Software Improvements Pty Ltd, eVACS® System Specification - Part 2 Scenario Analyses, version 1.1, 2020
7. Contract Change Proposals 1 to 9

    7.1 CCP1 – audio files to be WAV format

    7.2 Incorporated into 7.3

    7.3 Voting sequence to allow for Hide My Vote from ballot screen and same voting sequence for touchscreen and keypad operation

    7.4 Use password protect USBs for transfer of data

    7.5 Export of Pubic Key to support encryption of OSEV votes

    7.6 Allow multiple export of used voting tokens on a daily basis

    7.7 Include support for new keypads

    7.8 Include means to identify if drive has failed and secure means to replace failed drive

    7.9 Modifications to format of e-voting cards and polling place Administrator cards

2 Acronyms

Abbreviation or Term	Meaning
ACT	Australian Electoral Commission
ACT EC	ACT Electoral Commission
ASD	Australian Signals Directorate
CJB	Carol Boughton
CRS	Counting and Reporting Server
CSV	Comma-separated values
CVB	Clive Boughton
DEC	Data Entry Client
DEO	Data Entry Operator
DES	Data Entry Server
DESuper	Data Entry Supervisor
EACT	Elections ACT
eVACS / eVACS®	electronic Voting and Counting System
I-ESS-EC	Interface for Election Setup Server
I-VC-VS	Interface between Voting Client and Voting Server
IRS	Interface Requirements Specification
IVR	Interactive Voice Response
LAPPERDS	Legislative Assembly Polling Place and Election Results Display System
OCD	Operational Concept Description
OSEV	Overseas Electronic Voting
PPO	Polling Place Official
RAM	Random-Access Memory
RB	Russell Baird
SIPL	Software Improvements Pty Ltd
SRS	Software requirements Specification
SSS	System Specification
SSS-1-R	System Specification – Part 1 Requirements
SSS-2-SA	System Specification – Part 2 Scenario Analyses
TSV	Tab-Separated Values
TVS	Telephone Voting Server
UI	User Interface
USB	Universal Serial Bus
USB-FD	USB Flash Drive

3 Requirements

3.1 Introduction

eVACS® Upgraded is to be based on the functionality provided for the 2016 ACT Legislative Assembly election together with additional enhancements as reflected in new requirements.([1], [2] and [7]). The requirements for eVACS® Upgraded are therefore a combination of existing and new requirements.

The combined requirements are described in this Section 3, together with definitions of terms used in association with the requirements. A list of definitions with their page locations is at Table 1 and a list of the requirements with their page locations is at Table 2.

Section 3 has the following subsections:

Capability requirements

External interface requirements

Internal interface requirements

Internal data requirements

Safety requirements

Security and privacy requirements

Computer resource requirements

Design and construction constraints

Qualification provisions

3.2 System capability requirements

3.2.1 Overview of components

An installation of eVACS® to be used by Elections ACT for the 2020 Legislative Assembly Election includes the following software components:

- Election server, includes setup, data entry, counting and reporting functionality (one instance)
- Electronic voting client (many instances per polling place)
- Electronic voting server (one instance per polling place)
- Electronic telephone voting server (one instance)
- Interactive Voice Response platform for telephone voting (two instances)
- Data entry (many instances)

Except for telephone voting, all other software components are deployed individually; only one can ever be installed on any particular hardware at a time. For telephone voting, the inputs provided via a digital telephone are to be transferred via ‘voting client’ software to the telephone voting server, in the same manner as keystrokes are conveyed via the voting client to the voting server at polling places.

Note: Installing any of the eVACS® software components will delete any and all software existing on the hardware.

Table 1 - List of Definitions

Definition identifier	Defined item	Page
SSS-D-3-1	Election	16
SSS-D-3-2	Contest	16
SSS-D-3-3	Contest choice	16
SSS-D-3-4	Candidate choice	16
SSS-D-3-5	Voter	17
SSS-D-3-6	Ballot	17
SSS-D-3-7	Paper ballot	17
SSS-D-3-8	Electronic ballot	17
SSS-D-3-9	Vote	17
SSS-D-3-10	Paper vote	17
SSS-D-3-11	Electronic vote	17
SSS-D-3-12	Ballot type	17
SSS-D-3-13	Ballot rotation	18
SSS-D-3-14	Polling place	18
SSS-D-3-15	Vote normalisation	18
SSS-D-3-16	Unnormalised and normalised vote	18
SSS-D-3-17	Normalisation process	19
SSS-D-3-18	Counting system	19
SSS-D-3-19	Audit log	20
SSS-D-3-20	Error	21
SSS-D-3-21	Error message	21
SSS-D-3-22	Multiple languages	21
SSS-D-3-23	States of the voting client	25
SSS-D-3-24	Vote keystroke store	29
SSS-D-3-25	Vote touch screen store	29
SSS-D-3-26	Vote-in-progress store	29
SSS-D-3-27	Paper version number	31
SSS-D-3-28	Entry	32
SSS-D-3-29	Active Entry	32
SSS-D-3-30	Archived Entry	32
SSS-D-3-31	Data entry screen	32
SSS-D-3-32	Data control session	33
SSS-D-3-33	Data entry correction screens	33
SSS-D-3-34	Data control current contest	33
SSS-D-3-35	Data control current output device	33

Table 2 - 2020 List of Requirements

Requirement identifier	Defined item	Page
SSS-R-3.2-1	Ballots with rotation by permutation sequence	19
SSS-R-3.2-2	Voting server to manage use of sequences	19
SSS-R-3.2-3	Permutation used in sequence	19
SSS-R-3.2-4	Permuted display of control choices	19
SSS-R-3.2-5	Displaying a contest choice within a group	20
SSS-R-3.2-6	Electronic audit logs	20
SSS-R-3.2-7	Audit log entries timestamped	20
SSS-R-3.2-8	Audit log entries indicate origin	20
SSS-R-3.2-9	Access to audit log	20
SSS-R-3.2-10	Display error message on error	21
SSS-R-3.2-11	Display error message only on error	21
SSS-R-3.2-12	Errors logged to audit log	21
SSS-R-3.2-13	Error messages with recovery instructions	21
SSS-R-3.2-14	Error messages for voters and officials	21
SSS-R-3.2-15	Use of localised translation for display and printing	21
SSS-R-3.2-16	Installation erases disk contents	21
SSS-R-3.2-17	Election setup server initial menu	21
SSS-R-3.2-18	Loading from USB Flash Drive	22
SSS-R-3.2-19	Supported resolutions	22
SSS-R-3.2-20	Backup election data	22
SSS-R-3.2-21	Restore election data	22
SSS-R-3.2-22	One vote per barcode per contest	22
SSS-R-3.2-23	One vote per PIN/Voting Token pair per contest	23
SSS-R-3.2-24	Arrangement of candidates on an electronic ballot	23
SSS-R-3.2-25	Ballot legibility	23
SSS-R-3.2-26	Voting data stored twice	23
SSS-R-3.2-27	Voting data not to be stored with timestamp	23
SSS-R-3.2-28	Pre-polling backup	23
SSS-R-3.2-29	Spoken instructions	23
SSS-R-3.2-30	All formal votes accepted	23
SSS-R-3.2-31	Informal votes	23
SSS-R-3.2-32	Voting client response time	23
SSS-R-3.2-33	Barcodes to be QR codes	23
SSS-R-3.2-34	Avoid confusion between characters	24

SSS-R-3.2-72	Voting server menu during voting	30
SSS-R-3.2-73	Make two backups of voting server	20
SSS-R-3.2-74	Verifying voting server backups	30
SSS-R-3.2-75	Errors during writing backup of voting server	30
SSS-R-3.2-76	Generate and print QR codes for each voting server backup	30
SSS-R-3.2-77	Telephone voting server initial menu	30
SSS-R-3.2-78	Telephone voting server menu during voting	30
SSS-R-3.2-79	Make two backups of telephone voting server	31
SSS-R-3.2-80	Verifying telephone voting server backups	31
SSS-R-3.2-81	Errors during writing backup of telephone voting server	31
SSS-R-3.2-82	Data entry and counting servers installed	31
SSS-R-3.2-83	Data entry login screen	32
SSS-R-3.2-84	Vote entry screen	32
SSS-R-3.2-85	End vote screen	32
SSS-R-3.2-86	Cancel vote screen	32
SSS-R-3.2-87	Log data entry	33
SSS-R-3.2-88	Paper ballot entry client response time	33
SSS-R-3.2-89	Data entry correction and batch control menu	33
SSS-R-3.2-90	Vote control screen	34
SSS-R-3.2-91	End vote control screen	34
SSS-R-3.2-92	Cancel vote control screen	34
SSS-R-3.2-93	Integrate polling place votes	34
SSS-R-3.2-94	Integrate data entry votes	34
SSS-R-3.2-95	Export votes from data entry	34
SSS-R-3.2-96	Tag exported votes	34
SSS-R-3.2-97	Counting data backups	34
SSS-R-3.2-98	Counting audit	34
SSS-R-3.2-99	Intermediate results	34
SSS-R-3.2-100	Hare-Clark algorithm	35
SSS-R-3.2-101	Hare-Clark counting to provide for two counting options	35
SSS-R-3.2-102	Count by count scrutiny sheets	35
SSS-R-3.2-103	Counting of the choices	35
SSS-R-3.2-104	Distribution of effective votes	35
SSS-R-3.2-105	Tracking preferences	35
SSS-R-3.2-106	Counting - Less than 20 rule	35
SSS-R-3.4-1	Unicode	37

SSS-R-3.6-1	Voter anonymity	38
SSS-R-3.6-2	No public network	38
SSS-R-3.6-3	Vote data integrity and security	38
SSS-R-3.6-4	Access passwords to conform to Government requirements	38
SSS-R-3.6-5	ASD approved cryptographic protocols	38
SSS-R-3.6-6	Limit availability of ports on hardware	38
SSS-R-3.6-7	Hash code to be used when uploading votes to election server	38
SSS-R-3.7-1	Hardware supported by operating system	39
SSS-R-3.7-2	Election setup hardware	39
SSS-R-3.7-3	Electronic voting client hardware	39
SSS-R-3.7-4	With use of USB-FDs no longer applicable[	41
SSS-R-3.7-5	Operating system	41
SSS-R-3.7-6	Language of software shall be Ada	41
SSS-R-3.8-1	Independent code audit	41
SSS-R-3.8-2	Enhancements and legislative changes	41
SSS-R-3.9-1	Use of non-volatile storage on clients	41
SSS-R-3.10-1	Support for tests by officials	42

3.2.2 Election terminology

This section contains only definitions.

For an ACT Legislative Assembly Election currently there are five electorates each with a different ballot paper containing candidates representing different registered parties or independents, with five members to be elected for each electorate. The following definitions are those required to ensure accuracy in the development of an electronic voting, including telephone voting, eVACS® solution for ACT elections.

3.2.2.1 Elections

Definition SSS-D-3-1: Election

An election is a set of related contests. An election has the following properties:

Name: The name of the election.

Date: The date of the election.

Ballot type: See definition SSS-D-3-12

Rotation type: See definition SSS-D-3-13

Ballot instructions: Instructions on how to fill out an electronic ballot

Choice presentation: The format to be used for presenting candidate choices when displaying or describing a ballot.

Electorate type: The term used for an electorate in an election. In ACT Legislative Assembly elections ‘electorate’ is used; compare ‘divisions’ used in Federal House of Representative elections.

Contests: A set of contests

Definition SSS-D-3-2:Contest

A contest is a decision to be made by the voters associated with a particular electorate. A contest is a selection of candidates, currently five. Each contest has the following properties in addition to those associated with the ballot type (see definition SSS-D-3-12), the rotation type (see definition SSS-D-3-13), and the counting system (see definition SSS-D-3-18).

Electorate: The name of the electorate in which the contest is to be held.

Parties: A list of registered parties fielding candidates in the electorate.

Groups: A list of groups (either parties or independents listed in the same column on the ballot).

Choices: A list of contest choices (see definition SSS-D-3-3) for voters to select from.

In other words, an election specifies a number of contests – one per electorate – and the parameters common to all those contests.

In the ACT candidates not affiliated with a party are grouped into one or more groups labelled “Ungrouped”.

Definition SSS-D-3-3: Contest choice

A contest choice is a choice between candidates.

Definition SSS-D-3-4:Candidate Choice

A candidate choice is a person standing in a contest. Each candidate choice has the following properties:

Name: The name of the candidate

Party: The party to which the candidate belongs, if any

Group: The group to which the candidate is to appear on the ballot

Position: The canonical position within the group in which the candidate is to appear on the ballot

The Position property refers to 'canonical' position within the group.. However, the actual position used in the presentation of a particular ballot also depends on the rotation type (**SSS-D-3-13)** associated with the election.

Definition SSS-D-3-5: Voter

A voter is a person who casts a vote in a contest.

Eligibility to vote in a particular contest is beyond the scope of eVACS®.

3.2.2.2 Ballots and Votes

A ballot is the means by which a voter casts a vote in a contest. In eVACS®, there are two types of ballots: paper and electronic.

Definition SSS-D-3-6: Ballot

A ballot is either a paper ballot or an electronic ballot.

Definition SSS-D-3-7: Paper Ballot

A paper ballot is a piece of paper which can be used by a voter to make a vote in a contest.

Definition SSS-D-3-8: Electronic Ballot

An electronic ballot is a presentation by the eVACS® voting client software of an interface by which a voter can make a vote in a contest.

There are two types of electronic ballot: screen presentation with or without audio, and audio alone.

Definition SSS-D-3-9: Vote

A vote is either a paper vote or an electronic vote.

Definition SSS-D-3-10: Paper vote

A paper vote is the data generated by:

1. the eVACS® data entry client software as a result of a data entry operator entering the contents of a ballot paper, or
2. external software scanning a paper ballot.

Definition SSS-D-3-11: Electronic vote

An electronic vote is the data generated by the eVACS® voting client software as a result of a voter filling in an electronic ballot.

A vote completed as a result of a voter selecting keys on a telephone keypad or digital telephone in accordance with audio instructions is considered an electronic vote.

A vote completed via the Overseas Electronic Voting system is considered and electronic vote when uploaded to eVACS®,

3.2.2.3 Ballot type, vote formality, and interpretations and Votes

eVACS® must determine the formality of each vote so that only formal votes can be counted. It must also determine how a formal vote is to be interpreted during a count.

Definition SSS-D-3-12: Ballot type

Ballots for the ACT Legislative Assembly are of **Ranked Preference** type.

A number of candidates are to be marked with consecutive integers beginning with 1 (most preferred).

Minimum: The minimum number of candidates which must be marked for the electronic vote to be formal in the ACT is one (1).

Maximum: There is no maximum specified for the ACT.

Last preference implied: If there is only one candidate left on the ballot without a preference, then the last candidate is assumed to have received the last preference. Last preference implied is not used in the ACT.

3.2.2.4 Ballot rotation

In the ACT the ordering of contest options varies from ballot to ballot. This is referred to as Robson Rotation.

Definition SSS-D-3-13: Rotation by permutation sequence

Rotation of contest choices is performed with the use of a sequence of permutations.

Permutation sequence: A sequence of permutations in which the order of candidates are displayed within a group.

In the ACT with five members to be elected per electorate, the total number of Robson Rotation permutations is 60.

In general, parties usually field the maximum of five candidates; however, some parties and independents may have less than five in their group. In this case a reduced permutation is adopted. Should a party nominate more than 5 candidates, the candidates are spread as evenly as possible across multiple columns and the permutations apply separately to each column.

A mathematical description of permutations applicable to variable numbers is provided at Appendix A.

3.2.2.5 Polling places

Definition SSS-D-3-14: Polling place

A polling place is a location where voters may cast a vote in at least one contest; for the ACT Legislative Assembly Election a voter can only cast a vote in one contest. Each polling place has the following associated property:

Name: The name of the polling place.

As part of the process of setting up an election, polling places are defined, and sets of barcodes are generated for each polling place. Each barcode allows the casting of an electronic vote in a contest.

For telephone voting a single electronic polling place is established and instead of a barcode voters use a predetermined password/voting token combination to cast their vote.

The OSEV system is also identified as a single electronic polling place.

3.2.2.6 Vote interpretation

Once a vote has been entered it must be checked against the formality rules for the contest. If it is formal, it must also be normalised to make it suitable for counting.

Definition SSS-D-3-15: Vote normalisation

Vote normalisation is the process applied to a vote to transform it into a form which can be counted using the counting process for the contest.

Definition SSS-D-3-16: Unnormalised and normalised vote

Each vote cast in a contest exists in two forms: unnormalised and normalised. The unnormalised form contains the voter’s indications as expressed on the ballot; the normalised form is the result obtained by applying the vote normalisation process for the contest.

In the ACT a paper vote is accepted as formal as long as it contains a unique first preference, even though it may contain gaps in the numbering sequence or preferences which are duplicated. For example, a paper vote containing the preferences 1, 2, 3, 4, 4, 5, 6 in the normalisation process would keep the first three preferences and discard the rest.

Definition SSS-D-3-17: Normalisation process

A normalisation process is one of the following:

No normalisation - all vote preferences are left as is

Add last preference - last preference is inferred (not used in the ACT)

Remove gaps and duplicates – all preference beyond a gap in preferences or from a duplicate in a preference are removed, since the allocation of the next preference cannot be determined.

For example, if the preference sequence is: 1, 2, 3, 5, 6, then the candidate to receive the 4th preference is unknown and therefore the next preference after 3 cannot be assigned. Similarly, if the preference sequence is 1, 2, 3, 4, 4, 5, the next preference after 3 cannot be assigned.

3.2.2.7 Counting system

Definition SSS-D-3-18: Counting system

The counting system used for ACT Legislative Assembly elections is Hare-Clark (a type of electoral system of proportional representation using ranked preference ballots).

In an election using the Hare-Clark system, each contest has the following associated property:

Seats: The number of winners to be declared in the contest. For ACT, this is the number of members to be elected, currently five per contest (electorate).

3.2.3 Requirements on rotations

Requirement SSS-R-3.2-1: Ballots with rotation by permutation sequence

eVACS® supports ACT Legislative Assembly elections that use rotation of contest choices by permutation sequence.

Each voting server is responsible for issuing permutations to the voting clients that are connected to it. Permutations are issued by making a selection from the appropriate permutation sequence, treating the sequence as though it were a continuous loop.

Similarly, the telephone voting system is to provide the same functionality as a voting server at a polling place.

Requirement SSS-R-3.2-2: Voting server to manage use of sequences

Upon receipt of a request for a permutation for a contest from a voting client, a voting server shall issue the voting client with the permutation selected from the permutation sequence associated with that contest.

Requirement SSS-R-3.2-3: Permutation used in sequence

When a voting server selects a permutation from a permutation sequence, the permutation shall be:

- The first permutation in the sequence, if no client has previously requested a permutation from that sequence;
- The first permutation in the sequence, if the immediately preceding request for a permutation from that sequence resulted in the selection of the last permutation in the sequence;
- That permutation in the sequence which immediately follows the permutation most recently selected from that sequence, otherwise.

Requirement SSS-R-3.2-4: Permuted display of contest choices

When a voting client is required to display an electronic ballot which uses rotation by permutation sequence, the voting client shall, if and only if it has not previously done so during the current voting session, request the voting server to issue a permutation for the contest.

Requirement SSS-R-3.2-5: Displaying a contest choice within a group

When a voting client displays a contest choice as part of an electronic ballot which uses rotation by permutation sequence, the same rotation is used for the candidates within each group on the ballot paper.

For example, if the rotation order is 4, 3, 5, 2, 1 and there are 5 candidates standing, then for this ballot paper candidate 4 is in position 1, candidate 3 is in position 2, candidate 5 is in position 3, candidate 2 is in position 4 and candidate 1 is in position 5, where candidate numbering is based on their initial position on the ballot as drawn by the Electoral Commissioner.

If instead there are only three candidates in a particular group, then the order of presentation of these candidates based on the rotation order of 4, 3, 5, 2, 1 is candidate 3 in position1, candidate 2 in position 3, and candidate 1 in position 3.

Formally, the contest choice to be displayed shall be determined as follows with the above example to illustrate:

1. Let *p* be the permutation issued by the voting server for this contest for this voting session.[e.g. 4, 3, 5, 2, 1]
2. Let *c* be the total number of contest choices in the group in which the contest choice is to be displayed.[e.g. c = 3]
3. Let *i* be the screen position in which a contest choice is to be displayed (where the first position is 1 and the last is *c*) [e.g. positions 1, 2, 3]
4. The contest choice to be displayed in position *i* in the group is the contest choice of that group which has its Position property equal to *p(i)*.

hence, if the permutation for a particular ballot has the order 4, 3, 5, 2, 1 and the number of contest choices is only 3, then the order of presentation of the three candidates would be: 3 in position 1, 2 in position 2, 1 in position 3.

3.2.4 General Requirements

3.2.4.1 Auditing

Requirement SSS-R-3.2-6: Electronic audit logs

Every software component of eVACS® shall have the capacity to add auditing data to an electronic log.

Because of the physical separation of the components of eVACS®, the audit log is a distributed log. The following definition allows reference to logging without giving an indication of the physical location where a datum of audit information is stored.

Definition SSS-D-3-19: The audit log

The audit log is the collection of electronic audits maintained by all of the components in an installation of eVACS®.

Definition SSS-R-3.2-7: Audit log entries timestamped

Whenever an entry is made in the audit log a timestamp of when an entry was made shall be included in the entry, noting that committed votes are not to be time stamped.

Definition SSS-R-3.2-8: Audit log entries indicate origin

Whenever an entry is made in the audit log the entry shall identify the component of eVACS® which generated the entry.

Definition SSS-R-3.2-9: Access to the audit log

There shall be a capability for an authorised election official to generate a report of all audit data for each eVACS® component.

3.2.4.2 Errors and exceptions

Definition: SSS-D-3-20: Error

An error is any event or circumstance that prevents eVACS® from operating.

Definition: SSS-D-3-21: Error message

An error message is text that describes an error. Such text may be generic (i.e. Identical for each possible occurrence of an error), or contain a generic component as well as data specific to a particular occurrence of an error, as appropriate.

Definition: SSS-R-3.2-10: Display error message on error

When an error occurs eVACS® shall display an error message corresponding to that error.

Definition: SSS-R-3.2-11: Display error message only on error

eVACS® shall not display an error message unless an error has occurred.

Definition: SSS-R-3.2-12: Errors logged to audit log

When an error occurs a description of the error shall be added to the audit log.

Definition: SSS-R-3.2-13: Error messages with recovery instructions

An error message may either describe the steps to be taken to return eVACS® to operating condition, or give an index number by which the steps to be taken may be found.

Definition: SSS-R-3.2-14: Error messages for voters and officials

When eVACS® requires a voter or election official to take some action to correct an error the required steps shall be described in the error message.

When eVACS® requires a trained technician to take some action to correct an error, the error message may give only an index number by which the steps to be taken may be found.

3.2.4.3 Languages other than English

Definition: SSS-D-3-22: Multiple languages

eVACS® shall support multiple languages, including English, in respect of all written instructions and messages.

The particular languages available for a specific election is not pre-set, and is determined by Elections ACT for each election.

Note: Currently audio is only provided in English.

Requirement: SSS-R-3.2-15: Use of localised language for display and printing

Unless explicitly specified to the contrary, where a requirement or action includes text intended for display or printing, including instructions, that text shall be displayed or printed in a localised translation.

3.2.5 Election setup

Requirement: SSS-R-3.2-16: Installation erases disk contents

The process of installing the election setup server shall ensure that only software distributed as part of the election server setup software is installed concurrently on the same hardware.

[redacted]

[redacted]

Requirement: SSS-R-3.2-18: Loading from USB Flash Drive

When loading from USB Flash Drive (USB-FD) the user shall be prompted to insert the required USB-FD no more than three times. If the required USB-FD is not provided within the three attempts an error message shall be displayed that the USB-FD could not be loaded and the action requiring the USB-FD shall be aborted.

Requirement: SSS-R-3.2-19: Supported resolutions

Based on availability of all-in-one touch screens, a resolution of 1920 x 1080 is standard for a 23" screen.

The election server also has to be capable of displaying the ballot paper and preferably for the same resolution: 23" screen 1920 x 1080i

Requirement: SSS-R-3.2-20: Backup election data

The election server shall be capable of saving its state to a backup USB-FD

Requirement: SSS-R-3.2-21: Restore election data

The election server shall be capable of restoring its state from a backup USB-FD.

3.2.6 Electronic Voting

Requirement: SSS-R-3.2-22: One vote per barcode per contest

For any contest, the system shall not allow an individual barcode to be used to confirm more than one vote in the contest.

Requirement: SSS-R-3.2-23: One vote per PIN/Voting Token pair per contest

For any contest, the system shall not allow a PIN/Voting Token pair to be used to confirm more than one vote in the contest.

Requirement: SSS-R-3.2-24: Arrangement of candidates on an electronic ballot

When displaying an electronic ballot to a voter, the system shall display candidates in party groups as a column followed by column or columns of candidates who are not members of a registered party.

Requirement: SSS-R-3.2-25: Ballot legibility

The voting client shall display electronic ballots according to legibility guidelines.

Requirement: SSS-R-3.2-26: Voting data stored twice

eVACS® shall ensure that two copies of the electronic voting data are stored in separate locations within the polling place immediately after a vote is cast and confirmed by the voter.

Requirement: SSS-R-3.2-27: Voting data not to be stored with timestamp

eVACS® shall ensure that when a vote is stored in the votes database there shall be no timestamp associated with that transaction.

Note: There will still be a timestamp associated with a barcode or PIN/voting token pair being 'marked' as used.

Requirement: SSS-R-3.2-28: Pre-polling backup

eVACS® shall be capable of providing at the end of each day of the pre-polling period, electronic backup copies of voting data from each pre-polling centre.

Requirement: SSS-R-3.2-29: Spoken instructions

The electronic voting interface shall incorporate spoken instructions in English broadcast over disposable headphones for sight impaired people and for people with reading difficulties.

The telephone voting interface shall incorporate spoken instructions in English.

Requirement: SSS-R-3.2-30: All formal votes accepted

The voting client (for polling place and telephone voting) shall support the entering of any vote that is considered formal.

Requirement: SSS-R-3.2-31: Informal votes

The voting client (for polling place and telephone voting) shall support the entering of informal votes, in which no candidate has been selected.

Requirement: SSS-R-3.2-32: Voting client response time

After a vote is confirmed, eVACS® shall display the acceptance screen in a different colour for a specified time to be set the Elections ACT(subsequently set at 15 seconds). After that time expires, eVACS® shall be ready for the next voter within one second.

3.2.6.1 Barcodes

Requirement: SSS-R-3.2-33: Barcodes to be QR codes

2D barcodes, i.e. QR codes, are to be used for accessing voting terminals and casting votes, referred to as e-voting barcodes (that will be printed on e-voting cards).

A Master Admin QR code is to be required per polling place for use by a polling official to reset and shutdown voting terminals (instead of the previous key press sequences) and to access the menu functions on the polling place and telephone voting servers. Two copies to be printed, with one being a backup. One other Master Admin QR code is required to access the Election server.

A QR code of a SHA2 checksum (subsequently specified as SHA-256), to be generated with each export of votes from a polling place server (Master and Slave daily), is required for the upload of votes from voting servers (polling place and telephone voting) to the election server (see SSS-R-3.2-76).

[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

For QR codes used in conjunction with exported votes, when the files (from either the Master or Slave export) are read by the Election server a SHA2 checksum for the data in the files will be calculated and compared with the QR code accompanying those files:

1. If the two SHA2 checksums match, the vote data will be uploaded into temporary store and decrypted (for subsequent comparison with the other Master or Slave export)
2. If the two SHA2 checksums do not match, the vote data will be rejected and not loaded into temporary store.

3.2.6.2 Ballot legibility

Requirement: SSS-R-3.2-34: Avoid confusion between characters

Fonts used by the electronic voting client to display electronic ballots shall clearly distinguish characters that are likely to be confused.

For example, a font used to display English shall clearly distinguish between X and K, T and Y, I and L, I and 1, O and Q, O and 0, S and 5, and U and V.

3.2.6.3 Ballot flexibility

Requirement: SSS-R-3.2-35: Ability to vary font size within candidate name

The system is to provide configuration of the font size to be utilised when displaying the candidate name on the ballot screen.

3.2.6.4 Requirements specific to the voting client

Requirement: SSS-R-3.2-36: Provide flexibility in how text is programmed and displayed on screen

The system is to provide for configuration of fonts, font size and placement of text within the voting client display.

Requirement: SSS-R-3.2-37: Provide for touch screen functionality (in addition to separate keypad operations)

As a means for electors to navigate voting terminal touch screen functionality.

A graphical representation of the voting process, together with details of actions possible from each screen in the voting process and the text messages or instructions on each screen, is provided at Appendix B.

Requirement: SSS-R-3.2-38: Display screen with defined colours

Screen shall be displayed in the colours specified by the EACT, being:

Solids	Gradients
YELLOW SOLID = RGB 205 – 198 – 73	Dark orange - RGB 161 – 79 – 32
GREY SOLID = RGB 76 – 79 – 78	Light orange - RGB 169 – 99 – 37
	Dark purple - RGB 53 – 49 – 72
	Light purple - RGB 95 – 71 – 118
	Dark teal - RGB 40 – 74 – 78
	Light teal - RGB 90 – 127 – 145
	Dark grey - RGB 0 – 0 – 0
	Light grey - RGB 99 – 101 – 105

3.2.6.4.1 States

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]

[redacted] [redacted]

[redacted] [redacted]

3.2.6.4.2 Welcome Screen

Requirement: SSS-R-3.2-39

The Welcome Screen shall allow for the selection of language.

Requirement: SSS-R-3.2-40: Welcome screen properties: messages

The 'Welcome Screen' shall display or play a welcome message in the selected language.

The 'Welcome Screen' shall display a message acknowledging the traditional owners of the land in the selected language.

Requirement: SSS-R-3.2-41: Welcome screen properties: e-voting card instruction

The 'Welcome Screen' shall display or play an instruction to scan your e-voting card to start, in the selected language.

3.2.6.4.3 Main Voting Screen

Requirement: SSS-R-3.2-42: Main voting screen

The 'Main Voting Screen' shall allow the voter to select their preferred candidates and to hide their choices if they need assistance.

Requirement: SSS-R-3.2-43: Main voting screen properties: language

The 'Main Voting Screen' shall display instructions in voter's selected language.

Requirement: SSS-R-3.2-44: Main voting screen properties: groups

The 'Main Voting Screen' shall display each group for the electorate in a column, with the group assigned letter and name at the top, and one or more candidate names beneath it.

Requirement: SSS-R-3.2-45: Main voting screen properties: candidates

The 'Main Voting Screen' shall display each candidate in the column for his/her group.

Independent candidates are grouped in one or more columns, with the heading Ungrouped and no preceding letter.

Requirement: SSS-R-3.2-46: Main voting screen properties: display

The 'Main Voting Screen' shall display every group and every candidate for the electorate.

Requirement: SSS-R-3.2-47: Main voting screen properties: Zoom and Scroll

The 'Main Voting Screen' shall allow for zooming and scrolling to assist in displaying groups and candidates so they are easily visible.

Requirement: SSS-R-3.2-48: Main voting screen properties: Robson Rotation

The 'Main Voting Screen' shall display each group's candidates in the Robson Rotation order specified for the vote.

Requirement: SSS-R-3.2-49: Main voting screen properties: none

The 'Main Voting Screen' shall display each candidate name with an empty box to the left when no preferences have been entered.

Requirement: SSS-R-3.2-50: Main voting screen properties: preferences

If a vote contains a preference for a candidate, the 'Main Voting Screen' shall replace the empty box to the left of the candidate name with a coloured box containing the preference number for that candidate.

For touch screen preferences, the preference box or name of candidate shall be selectable by a single touch.

Requirement: SSS-R-3.2-51: Main voting screen properties: hide my vote

The 'Main Voting Screen' shall provide for the voter to 'hide their vote' with a message displayed and played to "Raise hand for help'.

3.2.6.4.4 Confirmation Screens

3.2.6.4.4.1 Confirmation screen with choices

Requirement: SSS-R-3.2-52: Confirmation screen

The 'Confirmation Screen' shall allow the voter to view and return to Main Voting screen to modify the current vote before concluding the voting session.

Requirement: SSS-R-3.2-53: Confirmation screen properties: language

The 'Confirmation Screen' shall display or play instructions in voter's preferred language.

Requirement: SSS-R-3.2-54: Confirmation screen properties: current vote

If the current vote is not empty, the 'Confirmation Screen' shall display and play only and all the candidates in the current vote, with the message such as 'Your choices in preference order are:'

Requirement: SSS-R-3.2-55: Confirmation screen properties: order

The 'Confirmation Screen' shall display those candidates in ascending order of the preference numbers in the boxes which were to their left on the 'Main Voting Screen'.

Requirement: SSS-R-3.2-56: Confirmation screen properties: instruction

If the current vote is not empty, the 'Confirmation Screen' shall display the instruction: "Review your choices " followed by 'To change your choices touch GO BACK. OR To confirm your choices scan your e-voting card.'

If the current vote is not empty the audio shall refer to UNDO to go back and to scan e-voting card (or enter PIN for telephone voting) to confirm preferences.

Requirement: SSS-R-3.2-57: Confirmation screen properties: hide my vote

The 'Confirmation Screen' shall provide for the voter to 'hide their vote' with a message displayed and played to "Raise hand for help'.

3.2.6.4.4.2 Confirmation screen with no choices (Informal vote screen)

Requirement: SSS-R-3.2-58: Confirmation screen properties: empty

If the current vote is empty, the 'Informal Vote Screen' shall be displayed with messages and audio such as 'You have not selected any candidates. Do you want to cast a blank informal vote/" with the choices:

No I want to return to the ballot paper. Touch GO BACK or press SELECT (5) to continue selecting candidates

Yes I want to cast a blank informal vote. Touch CAST AN INFORMAL VOTE or press FINISH (#) to continue.

3.2.6.4.4.3 Reconfirm and scan screen with no choices

Requirement: SSS-R-3.1-59: Reconfirm & scan screen properties: instruction

If CAST AN INFORMAL VOTE is selected on the Informal Vote screen, the 'Reconfirm & Scan Screen shall be displayed with:

Nearly there …

Scan your e-voting card now to cast your informal vote

OR

To return to the ballot paper, touch GO BACK

Audio instructions refer to pressing UNDO (*) to go back or scan e-voting card to cast vote (or enter PIN for telephone voting).

3.2.6.4.5 Hidden Vote Screen

Requirement: SSS-R-3.2-60: Hidden vote screen

The 'Hidden Vote Screen' shall hide the voter's current vote.

Requirement: SSS-R-3.2-61: Hidden vote screen properties: language

The 'Hidden Vote Screen' shall display instructions in the voter's preferred language.

Requirement: SSS-R-3.2-62: Hidden vote screen properties: message

The 'Hidden Vote Screen' shall display the message; "Your vote is now hidden. Raise your hand if you need help. An e-voting officer will be with you shortly"

With the option to CONTINUE VOTING if voter arrived at Hidden Vote screen from Main Voting screen.

With options to CONTINUE VOTING or scan e-voting card if voter arrived at Hidden Vote screen from Confirmation screen.

3.2.6.4.6 Start Again Screen (Clear Choices screen)

Requirement: SSS-R-3.2-63: Start again screen

The 'Start Again Screen' shall allow the voter the option to clear the Vote-in-Progress and enter a new set of preferences.

Requirement: SSS-R-3.2-64: Start again screen properties: language

The 'Start Again Screen' will be displayed in the voter's preferred language.

Requirement: SSS-R-3.2-65: Start again screen properties: message

The 'Start Again Screen' will display and/or play the question "Are you sure you want to clear all preferences and start again? With the choice of Yes or No.

3.2.6.4.7 Acknowledgement Screen (Acceptance screen)

Requirement: SSS-R-3.2-66: Acknowledgement screen

The 'Acknowledgement Screen' shall appear on conclusion of the voting session.

Requirement: SSS-R-3.2-67: Acknowledgement screen properties: language

The 'Acknowledgement Screen' message will be in the voter's preferred language.

Requirement: SSS-R-3.2-68: Acknowledgement screen properties: message

The ‘Acknowledgement Screen’ will display and/or play the message: “Your vote has been accepted. Please place your e-voting card in the ballot box on your way out of the polling place.”

Requirement: SSS-R-3.2-69: Acknowledgment screen properties: colour

Acknowledgement screen colour to be different to that of other screens so that polling official can easily see that the voter has scanned their e-voting card a second time (subsequent decision to be pink).

3.2.6.4.8 [redacted]

[redacted]

[redacted]

[redacted]

3.2.6.4.9 Reset

Requirement: SSS-R-3.2-70: Reset

The voting client shall allow the reset of the voting process.

3.2.6.5 Requirements specific to the polling place voting server

(see section 3.2.7 for telephone voting server)

[redacted]

- [redacted]
    - [redacted]
- [redacted]

[redacted]

Requirement: SSS-R-3.2-73: Make two backups of voting server

The voting server shall allow a polling official to produce two removable, complete backups containing all confirmed votes stored on the server.

Requirement: SSS-R-3.2-74: Verifying voting server backups

After writing a backup of votes stored on a voting server, the backup shall be verified to determine if the removable medium can be read without errors and the data stored in the backup matches the original data stored on the server.

Requirement: SSS-R-3.2-75: Errors during writing backup of voting server

If the backup verification of a voting server indicates that the removable medium cannot be read without errors, or if the data stored on the medium does not match the original data stored on the server, the voting server shall not consider that the medium to be one of the two backups referred to in requirement SSS-R-3.2-45.

Requirement: SSS-R-3.2-76: Generate and print QR codes for each voting server backup of votes

The voting server shall create a SHA2 hash for each backup and print as a QR code.

3.2.7 Telephone voting

[redacted]

[redacted]

[redacted] [redacted]

Requirement: SSS-R-3.2-79: Make two backups of telephone voting server

The telephone voting server shall allow a polling official to produce two removable, complete backups containing all confirmed votes stored on the server.

Requirement: SSS-R-3.2-80: Verifying telephone voting server backups

After writing a backup of votes stored on the telephone voting server, the backup shall be verified to determine if the removable medium can be read without errors and the data stored in the backup matches the original data stored on the server.

Requirement: SSS-R-3.2-81: Errors during writing backup of telephone voting server

If the backup verification of a voting server indicates that the removable medium cannot be read without errors, or if the data stored on the medium does not match the original data stored on the server, the voting server shall not consider that the medium to be one of the two backups referred to in requirement SSS-R-3.2-45.

3.2.7.1 [redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

3.2.8 [redacted]

[redacted]

[redacted]

[redacted] of paper ballots using a screen layout that matches the layout of the ballot as it was printed.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] to start again (by clearing the preferences) and shall offer the two possible answers ‘Yes’ and ‘No’.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

3.2.9 [redacted]

[redacted]

[redacted]

[redacted]

[redacted] data entry server to removable media, the exported data shall be identifiable as a data entered vote.

3.2.10 Electronic voting counting and reporting

Requirements relating to counting and reporting processes are specific to the ACT Legislative Assembly elections application of the Hare-Clark election system.

Requirement: SSS-R-3.2-97: Counting data backups

eVACS® shall maintain a complete backup and support restoration of all configurations information relayed to or captured by the vote counting and reporting system.

Requirement: SSS-R-3.2-98: Counting audit

Information regarding the counting process and generation of election results shall be logged to the audit log. Such information shall include: results of intermediate counts, candidates eliminated (before a redistribution of preferences), and decisions made by officials required as part of the counting process e.g. the outcome of a tie.

Requirement: SSS-R-3.2-99: Intermediate results

The counting system shall be capable of generating an intermediate election result at any point during counting from the set of votes deemed to be valid at that time.

Requirement: SSS-R-3.2-100: Hare-Clark counting algorithm

The counting system shall support generation of election results for multiple-member electorates and a casual vacancy through the use of Hare-Clark counting, to be implemented via 'stored procedures'.

Requirement: SSS-R-3.2-101: Hare-Clark counting to provide for two counting options

eVACS® to provide for the option to select:

i) Vote values calculated by multiplying ballot paper totals by fractional transfer values rounded down to 6 decimal places, and

ii) Vote values calculated by multiplying ballot paper totals by fractional transfer values rounded down to the nearest whole number.

Requirement: SSS-R-3.2-102: Count by count scrutiny sheets

The reporting system shall be capable of producing scrutiny sheets detailing the count-by-count progress for each contest.

Requirement: SSS-R-3.2-103: Counting of the choices

The reporting system shall be capable of producing a 'Counting of the choices' scrutineering report for a completed election result. (referred to as Table I).

Requirement: SSS-R-3.2-104: Distribution of effective votes

The reporting system shall be capable of producing a 'Distribution of effective votes' scrutineering report for a completed election result (referred to as Table II).

Requirement: SSS-R-3.2-105: Tracking of preferences

The reporting system shall be capable of producing a report which tracks the movement of each vote between counts.

Requirement: SSS-R-3.2-106: Counting – less than 20 votes

The reporting system shall not display and/or print results where there are less than 20 votes in total for a polling place/electorate category.

3.3 System interface requirements

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

3.4 System internal data requirements

Requirement: SSS-R-3.4-1: Unicode

All text imported, exported, and stored by eVACS® shall be encoded in Unicode; latest available version is 12.0. [5] [6]

3.5 Safety requirements

In order to provide a safe operating environment, computer hardware deployed as part of an eVACS® installation should satisfy relevant legislation requirements regarding safety. These requirements are beyond the scope of this document.

3.6 Security and privacy requirements

In existing paper ballot systems, each ballot paper is the authorisation and the means by which a vote is cast. In electronic voting using eVACS®, each barcode or PIN/Voting Token pair has a similar role. In general, neither a ballot paper nor barcode nor voting token can be issued to a potential voter unless and until their eligibility to vote has been determined. There is a separate process to deal with Declaration votes.

The consequence of this is that all transfers of barcode or voting token data must be secured. For barcodes this includes delivery of the barcode data to a printing facility, the supervision of the printing process and delivery of the printed barcodes to the polling places. No barcode information should be retained at any printing facility.

The processes of allocation of barcodes to polling places and their delivery should reflect the same security processes employed for the distribution of paper ballots.

Each created polling place and telephone voting server contains barcode and PIN/Voting Token data and therefore must be securely delivered and kept secure on delivery.

To undertake User Acceptance Testing of eVACS®, EACT internally prints barcodes to be used for that testing. Since the same process is used to create pdfs for printing barcodes either internally or externally 'Test' barcodes cannot be identified as such. Care is therefore required in keeping secure the barcodes printed for internal testing.

Voting tokens are generated within eVACS® and are exported for assignment to registered telephone voters within the external TIGER system. Registered telephone voters have provided a private Personal identification Number (PIN) as part of the registration process and TIGER is required to generate a list of PIN/voting token pairs on a regular basis to be uploaded into the Telephone Voting Server on a regular basis. Throughout this process the security of the telephone voting tokens must be maintained to the same level of protection as ballot papers.

Each voting server, polling place and telephone voting, exports vote data to USB-FDs as part of backup processes; these must be delivered securely to the location of the counting server.

The following list summarises the required security policies.

Barcode data generated from setup process

- Secure transport between setup and printing facility
- No barcode data retained at printing facility

Printed barcodes

- Secure transport between printing facility and election officials
- Secure delivery to, and storage at, electronic voting centres
- No barcode issued to a voter unless and until eligibility to vote has been confirmed

USB-FDs containing backups of voting server, polling place and telephone voting

- Use of encrypted container on USB-FDs used for transferring votes
- Secure delivery to and from voting server

Voting tokens generated from setup process

- Use of encrypted container on UDB-FD for secure transfer to system assigning tokens
- Voting tokens randomly assigned to registered telephone voters on electorate basis

USB-FDs containing PIN/voting token pairs

- Secure delivery to telephone voting server

Requirement SSS-R-3.6-1: Voter anonymity

The system shall protect the anonymity of each voter, including the shuffling of votes in the database.

Requirement SSS-R-3.6-2: No public network

The system shall not be connected to any outside network in any of the electronically equipped polling places, and the central scrutiny centre.

Requirement SSS-R-3.6-3: Vote data integrity and security

The system shall allow for votes data to be transferred to the vote counting system without accidentally or deliberately being altered.

Requirement SSS-R-3.6-4: Access passwords to conform to Government requirements

Passwords throughout the system should only be able to be set if they meet ACT Government and ASD password security standards.

Requirement SSS-R-3.6-5: ASD approved cryptographic protocols

Only ASD approved cryptographic protocols to be used throughout the system, I.e. TLS1.2 and SHA2.

Requirement SSS-R-3.6-6: Limit availability of ports on hardware

All unused ports on server and client components shall be decommissioned via the operating system.

3.6.1 Requirement to be satisfied by a system component

Requirement SSS-R-3.6-7: Hash code to be used when uploading votes to election server

To import data from the voting servers into the election server, the system is to mandate the entry of the hash code (in QR code format) on the election server.

3.7 Computer resource requirements

The descriptions provided in this section serve as a base definition of support for the operation of eVACS®. Each requirement referring to a particular item of hardware or software is more properly interpreted as a constraint on the design of eVACS®.

3.7.1 Hardware requirements

The components of eVACS® are designed to operate on off-the-shelf hardware. Except where otherwise specified, the following specifications are to be regarded as minimums. In addition, only components support by the required operating system are to be used (see SSS-R-3.7-5)

Requirement SSS-R-3.7-1 Hardware supported by operating system

Where a hardware component is listed as a requirement, that hardware component shall also be supported by the required operating system.

3.7.1.1 Election servers

Requirement SSS-R-3.7-2 Election setup - hardware for servers

The election server hardware shall at a minimum consist of the following:

- Intel architecture i5/i7
- 8 GB main memory
- PC-type keyboard
- 256 GB hard disk drive
- USB ports (at least three for keyboard, scanner and printer)
- Ethernet card 802.3

Plus

- USB connected PCL Printer for A3 printing
- Screen appropriate to view menu and preview ballot (1920 x 1080 resolution)

For polling place server or telephone voting server, same as for election server with the following changes:

- 16 GB instead of 8 GB main memory
- Additional 256 GB hard disk drive
- 2D barcode reader (scanner)
- PCL printer for A4 printing
- Screen to view menus

3.7.1.2 Electronic ‘clients’

Requirement SSS-R-3.7-3 Electronic voting client hardware

The electronic voting client hardware shall consist of the following:

- Intel architecture i5
- 4 GB main memory
- USB port (for scanner)
- Ethernet 802.3

If a client is to support touchscreen functionality, it shall also consist of:

- 23” touch screen display supporting 1920 x 1080 resolution and single touch
- A scanner

Note: voting client is expected to be an All-in-One

If a vision-impaired client, i.e. supporting voting by blind or vision-impaired voters, it shall also have:

- Audio capability
- Headphones
- Telephone-style keypad
- A scanner

The functionality of the telephone-style keypad is as shown in Figure 2. The functionality for telephone voting while similar has differences, as shown in Figure 3.

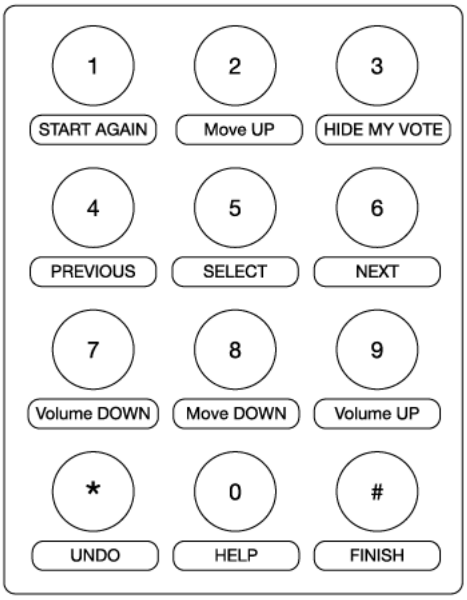

Figure 2 - Keypad functions for BV&I setup at polling places

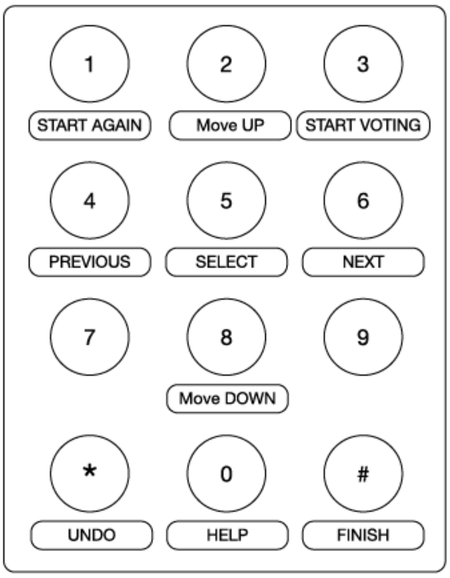

Figure 3 - Key functions for telephone voting

Data entry client

Same as for voting client

The functionality of the keypad (standard keyboard with numeric keypad with NUM LOCK On) used for data entry is as shown in Figure 4.

	FINISH	CANCEL	↑
7	8	9	NEXT GROUP
4	5	6	
1	2	3	
0		DELETE **YES**	↓ / NO

Figure 4 - Key pad for data entry

Vote storage

Officials must ensure cleansed, and if available write once, media is used for transporting and storing vote data.

Requirement SSS-R-3.7-4 Voter data media finalised

Requirement applied to use of CD/DVD and is not applicable to USB-FDs.

Computer software requirements

Requirement SSS-R-3.7-5 operating system

Each of the computers to be used for eVACS® shall be capable of operating with the Linux operating system.

Requirement SSS-R-3.7-6 Language of software to be Ada

eVACS® upgraded shall be written in Ada, current version being Ada 2012.

3.8 System quality factors

Requirement SSS-R-3.8-1 Independent code audit

The system shall allow programming code to be independently audited and be available to scrutineers for verification.

Requirement SSS-R-3.8-2 Enhancements and legislative changes

The system shall be capable of amendment to cater for enhancement and legislative changes.

3.9 Design and construction constraints

3.9.1 Voting client

Requirement SSS-R-3.9-1 Use of non-volatile storage on voting client

The voting client shall not store electorate, candidate, or vote data in its non-volatile storage.

This constraint nevertheless permits a voting client to cache such data in its non-volatile storage (i.e., in RAM)

3.9.2 Training related requirements

All training and development of training materials is undertaken by EACT officials.

3.9.3 Logistic related requirement

As rotation of ballot papers is used in ACT Legislative Assembly Elections, every paper ballot for that election must have a rotation number printed on it; this rotation number is entered before data entry of the ballot details as part of the data entry process.

3.10 Qualifications provisions

Requirement SSS-R-3.10-1 Support for tests by officials

The system shall be capable of being tested by EACT officials under load conditions to the satisfaction of officials prior to acceptance of the system.

4 Requirements traceability

A separate matrix traces requirements through the various development documents.

Appendix A - Permutation explanations

Permutation

In general terms a permutation is one of several possible ways in which a set of numbers or things can be ordered or arranged.

For example, if there are three numbers 1, 2 and 3, then these can be arranged in order to give 6 possible permutations:

1 2 3, 1 3 2, 2 1 3, 2 3 1, 3 1 2, and 3 2 1

This can be expressed mathematically as follows.

A permutation of the numbers 1 …*n* is a function $p : \{ 1, \ldots, n\} \to \{ 1, \ldots, n\}$ which is a bijection*.

For example, the function $\{ 1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 2, 5 \mapsto 1\}$ is a permutation of the numbers 1 *n*, where *n* = 5, but the function $\{ 1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 1\}$ is not because although the numbers 1 to 5 are part of the first set, the mapped set does not correspond, having 1, 3, 3, 4, 5 instead.

*Bijection is a ‘mapping’ that is both one-to-one (an injection) and onto (a surjection), i.e. a function which relates each member of a set *S* (the domain) to a separate and distinct member of another set *T* (the range), where each member in *T* also has a corresponding member in *S*.

Size of Permutation

If p is a permutation of the numbers 1…*n*, the size of p , denoted by size(p), is *n*.

If an election uses rotation by permutation sequence, displaying an electronic ballot involves arranging the contest choices in each group in an order determined by a permutation selected from the permutation sequences for the contest.

Because the number of contest choices in a group may not be equal to the size of the permutation, the choices are arranged using a reduced permutation.

Given a permutation p and a number *c* which is less than or equal to the size of *p*, the reduced permutation of *p* to size *c*, denoted p_c , is the permutation of the numbers 1…*c* calculated according to the following algorithm:

```
1. Set $i \to 1$ and $j \to 1$
2. Set $p_c \to \{ \}$
3. While $i \leq$ size($p$):
    3.1. If $p(i) \leq c$ then:
        3.1.1. Set $p_c \to p_c \to \{ j \mapsto p(i)\}$
        3.1.2. Set $j \to j+1$
    3.2. Set $i \to i+1$
```

For example, if $p = \{ 1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 2, 5 \mapsto 1\}$, then:

$$p_5 = \{ 1 \mapsto 3, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 2, 5 \mapsto 1\}$$

$$p_4 = \{ 1 \mapsto 3, 2 \mapsto 4, 3 \mapsto 2, 4 \mapsto 1\}$$

$$p_3 = \{ 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1\}$$

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

– End of Document –