X-HAT DIGITAL VOTING PLATFORM

PRELIMINARY TECHNICAL INCIDENT, SYSTEM PERFORMANCE AND ELECTION IMPACT REPORT

Prepared for: University of Fort Hare

Prepared by: Black Hat Group

Project: X-HAT Digital Voting Web Application – SRC Elections

Technical role: Platform Development, Deployment and Hosting

Platform: https://x-hat.co.za

Voting locations: Alice and East London campuses

Report classification: Technical and Operational Accountability Report

1. EXECUTIVE SUMMARY

The X-HAT Digital Voting Platform was developed and deployed to facilitate the University of Fort Hare's Student Representative Council (SRC) electoral process through a centralised digital voting environment.

The platform was designed to provide eligible students with access to electronic voting, student verification, OTP-based authentication, ballot submission and centralised recording of voting transactions. It also provided administrative functionality to monitor participation and manage the electoral process.

During the voting exercise, the platform experienced several technical interruptions that affected different components of the system. These included an initial time synchronisation discrepancy, network accessibility challenges on the university's Wi-Fi infrastructure, and significant disruptions to the email authentication service following the suspension of the original Mailchimp account.

The most significant challenge arose from the dependency on third-party email infrastructure for OTP delivery. Following the suspension of the original Mailchimp account, the technical team had to establish alternative email delivery arrangements while the election was already in progress.

The transition involved several complications, including:

- Limited email sending capacity on the existing cPanel environment.
- Delays in activating the replacement Mailchimp account on a paid subscription.
- Restrictions imposed on the replacement account's trial version.

- An unsuccessful attempt to establish an SMTP connection with the university's email server.
- DNS configuration and propagation delays.
- Students using personal Gmail accounts who were unable to receive their OTP verification emails and consequently could not proceed to vote.

These challenges resulted in temporary interruptions to the voting process and affected the ability of some eligible students to participate.

The technical team responded to the incidents through investigation, configuration adjustments, alternative service arrangements and continuous engagement with the University's ICT Department and external service providers.

Following the final restoration of the email configuration, the platform operated without further reported technical glitches until the official closure of voting.

This report provides a chronological account of the incidents, their causes, corrective interventions, estimated downtime, implications for voter participation, potential effects on election results and recommendations for improving the resilience of future digital elections.

An important distinction is made throughout this report between website availability, authentication service availability and the integrity of successfully recorded votes. These are separate technical considerations and should be assessed independently.

2. PURPOSE AND OBJECTIVES OF THE REPORT

The purpose of this report is to provide the University of Fort Hare with a transparent and comprehensive account of the technical challenges experienced during the X-HAT digital voting exercise.

The report seeks to:

1. Document the system glitches and technical incidents experienced during voting.
2. Establish the approximate duration of identified interruptions.
3. Explain the technical causes of the incidents, distinguishing confirmed findings from possible contributing factors.
4. Account for corrective measures implemented by the technical team.
5. Explain how the incidents affected students' ability to access the platform and complete voting.
6. Highlight the implications of OTP delivery failures, including those affecting Gmail users.

7. Assess potential implications for voter turnout and the overall election results.
8. Recommend technical and operational improvements for future elections.
9. Establish the importance of reconciling voting records and preserving system audit evidence.

3. OVERVIEW OF THE X-HAT DIGITAL VOTING PLATFORM

The X-HAT platform was developed to provide a digital alternative to conventional voting processes, enabling students to participate electronically while allowing election administrators to monitor and manage voting activities.

The system incorporated the following functionalities:

System component	Description
Student verification	Checks student information against the institutional database supplied by the university.
OTP authentication	Sends verification codes to students' registered email addresses.
Voter eligibility	Determines whether a student exists in the supplied student database and is eligible to proceed.
Electronic ballot	Provides the interface through which eligible students cast their votes.
Voting status	Updates the student's voting status following successful submission.
Database management	Stores student records and voting transactions.
Administrative dashboard	Provides election administrators with system management and monitoring functionality.
Reporting	Supports the extraction and review of voting information.
Query management	Provides a channel for handling student queries and election-related concerns.

3.1 Authentication and voting process

The authentication process relied on the student information supplied by the university, together with email-based OTP verification.

The general process was as follows:

1. A student accesses the X-HAT website.
2. The student enters the required identification information.
3. The system checks the student's details against the university's student database.
4. Where the student is recognised and eligible, an OTP is generated and sent to the registered email address.
5. The student enters the OTP to complete authentication.
6. The student proceeds to the electronic ballot.
7. Upon successful submission, the voting transaction is recorded and the student's voting status is updated.

The email authentication mechanism was therefore a critical dependency.

Even where the website and database were operational, a student who could not receive the OTP could not complete authentication and proceed to vote.

This distinction is particularly important when assessing the impact of the email delivery incidents.

4. CHRONOLOGICAL ACCOUNT OF TECHNICAL INCIDENTS

This section provides the sequence of events as experienced during the voting exercise, including the technical challenges, investigations and interventions undertaken.

4.1 Incident 1: Delayed commencement of voting due to time synchronisation

20-minute delay

Resolved

Description of incident

At the scheduled opening of voting, the platform initially failed to accept votes as expected. Students attempting to participate at the official opening time could not proceed with the voting process.

The technical team immediately investigated the issue to establish whether it was related to the application, database connectivity or voting configuration.

Root cause identified

Upon investigation, the team discovered that the time settings on the application environment were not aligned with those configured on the database.

This discrepancy resulted in the system interpreting the voting opening time incorrectly.

Since the voting application relied on time-based conditions to determine when voting could commence, the difference between the two environments prevented the system from accepting votes at the scheduled time.

Corrective measures

The technical team:

- Investigated the application and database time configurations.
- Identified the discrepancy in the respective time settings.
- Corrected the configuration to ensure consistency.
- Tested the voting functionality.
- Confirmed that the system could accept voting submissions.

Impact on the voting process

The commencement of voting was delayed by approximately 20 minutes.

Students were temporarily unable to cast their votes during this period. The incident affected the planned start of the election but was resolved, allowing the voting process to continue.

Preventative recommendation

Future deployments should incorporate automated Network Time Protocol (NTP) synchronisation, consistent timezone settings, and pre-election testing of the opening and closing conditions.

4.2 Incident 2: University Wi-Fi connectivity and domain accessibility

Approximately 30 minutes

Resolved with UFH ICT

Description of incident

Following the resolution of the initial time-setting issue, the platform operated successfully for approximately one and a half hours.

Thereafter, the technical team began receiving reports from students who could not access the X-HAT domain when connected to the University's Wi-Fi network.

The investigation established an important difference in accessibility:

- Students connected to the university Wi-Fi network experienced difficulties accessing x-hat.co.za.
- Students using mobile data were able to access the platform successfully.
- The issue appeared to be isolated to the university's network environment rather than a general outage of the X-HAT website.

Investigation and root cause assessment

The technical team conducted connectivity checks using alternative internet connections.

The fact that mobile data users could access the platform indicated that the issue was potentially associated with the university's network infrastructure.

Possible contributing factors included:

- DNS resolution problems.
- Firewall restrictions.
- Domain or web-filtering policies.
- Network routing or connectivity configuration.

The exact underlying network configuration responsible for the issue was not independently established during the incident.

Corrective measures

The technical team immediately escalated the matter to the University's ICT Department.

The university ICT representative acknowledged the issue and confirmed the need for investigation.

The technical team continued monitoring accessibility while engaging the university's ICT personnel.

After approximately 30 minutes, connectivity was restored, and students could once again access the X-HAT domain through the university Wi-Fi network.

Impact on the voting process

The incident temporarily disadvantaged students who depended on university-provided Wi-Fi to access the voting platform.

Although students using mobile data could continue accessing the system, those relying on campus connectivity experienced difficulties participating.

This created unequal access conditions during the affected period and temporarily disrupted the voting process.

Preventative recommendation

The university should undertake domain whitelisting, DNS verification, firewall assessments and network compatibility testing before future elections.

A formal network access confirmation should be obtained from the ICT Department before voting commences.

4.3 Incident 3: Suspension of the original Mailchimp account

Major authentication disruption

Appeal pending

Description of incident

After the university Wi-Fi accessibility issue had been resolved, the voting platform continued operating for approximately three hours.

During this period, the technical team encountered a significant disruption when the Mailchimp account used for bulk OTP email delivery was suspended.

The suspension followed an automated suspicious-activity assessment conducted by Mailchimp's abuse-prevention system, Omnivore.

The account was subsequently disabled, preventing the technical team from continuing to use the original email delivery service.

Root cause

The suspension was initiated by Mailchimp's automated abuse-prevention mechanisms.

The suspension was an external service-provider intervention and not a confirmed failure of the X-HAT application or voting database.

The technical team submitted a formal appeal requesting that Mailchimp review the account and restore its services.

However, the appeal was not resolved immediately and remained pending during the reporting period.

Corrective measures

To avoid a prolonged interruption, the technical team immediately explored alternative email delivery arrangements.

The existing cPanel email infrastructure was activated as an alternative mechanism for sending OTP verification codes.

However, this presented another operational challenge because the cPanel environment had a significantly lower sending capacity than the requirements of the election.

The available sending capacity was approximately 400 emails per hour.

This was insufficient for an electoral process involving a large student population requiring authentication within a limited period.

Impact on the voting process

The Mailchimp suspension interrupted the OTP delivery mechanism.

Students who needed to authenticate during this period could experience delays or fail to receive their verification codes.

Although the voting website and database were separate from the Mailchimp service, the suspension affected students' ability to complete authentication and access the ballot.

This incident highlighted the risks associated with relying on a single external email delivery provider for a high-volume institutional voting exercise.

4.4 Incident 4: Transition to a replacement Mailchimp account

Approximately 45 minutes

Alternative arrangement implemented

Description of incident

Following the suspension of the original Mailchimp account, the technical team initiated the creation of a replacement account to restore bulk email delivery.

The intention was to establish an alternative service with sufficient capacity to support the remaining voting period.

However, the replacement account had not yet been activated on the required paid subscription and remained on its trial configuration.

The trial account only processed approximately 500 emails before reaching its sending restriction.

This resulted in another interruption to OTP delivery.

Corrective measures

The technical team:

- Created a replacement Mailchimp account.
- Initiated the required account configuration and migration process.
- Attempted to activate the appropriate paid subscription.

- Tested the email delivery functionality.
- Identified that the replacement account remained subject to trial restrictions.
- Continued investigating alternative email delivery arrangements.

The transition process resulted in approximately 45 minutes of disruption.

Impact on the voting process

Students requiring OTP authentication during the transition period may have experienced delayed or unsuccessful delivery of verification codes.

The issue also increased operational pressure because the electoral process was already underway and students were actively attempting to vote.

The incident demonstrated the importance of having a fully activated and tested backup email service before an election begins.

4.5 Incident 5: Attempted integration with the University SMTP server

Unsuccessful integration

Description of incident

As an alternative to relying on external email service providers, the technical team engaged the University's ICT Department to explore the possibility of sending OTP emails through the university's institutional SMTP server.

The objective was to establish a direct email delivery channel between the X-HAT hosting environment and the university's institutional email infrastructure.

The team attempted to configure the connection using the university SMTP server details.

However, the connection could not be established successfully during the voting exercise.

Technical considerations

An institutional SMTP integration generally requires:

- An approved SMTP hostname and port.
- Appropriate authentication credentials or authorised relay permissions.
- Firewall approval for outbound SMTP traffic.
- Public IP whitelisting where required.
- TLS/SSL configuration.
- Authorisation to send using the institutional email domain.

- Confirmation of sending limits and security controls.

The inability to establish the connection meant that the university's email infrastructure could not be used as an immediate replacement for the suspended Mailchimp service.

Corrective measures

The technical team continued engaging UFH ICT while maintaining the cPanel email arrangement as an alternative.

The team also continued communicating with Mailchimp technical support in an effort to restore the preferred email delivery configuration.

Impact on the voting process

The unsuccessful SMTP integration delayed the availability of an alternative institutional email delivery channel.

This prolonged the authentication challenges and required the technical team to continue working with the available email infrastructure.

4.6 Incident 6: Reversion to cPanel and DNS propagation

Approximately 30-minute restoration period

Restored

Description of incident

Following the restrictions encountered on the replacement Mailchimp account and the unsuccessful university SMTP integration, the technical team reverted to the existing cPanel email delivery arrangement.

This was done while communication with Mailchimp technical support continued.

During the process, the team monitored the DNS configuration associated with the transition to the alternative email service.

The updated DNS settings required time to propagate across the relevant DNS infrastructure.

Approximately 30 minutes later, the DNS changes had propagated, allowing the revised email configuration to become operational.

Corrective measures

The technical team:

- Reverted to the available cPanel email delivery configuration.
- Continued monitoring email delivery.

- Maintained communication with Mailchimp technical support.
- Monitored the DNS configuration and propagation.
- Verified restoration of the required email functionality.
- Continued monitoring the voting platform.

Impact on the voting process

The transition and DNS propagation period resulted in further delays to OTP email delivery.

The technical team had to manage the available email capacity while working to restore the preferred email delivery arrangement.

Once the configuration was restored, the platform continued operating without further reported technical glitches until the official closure of voting.

4.7 Incident 7: OTP delivery failures affecting students using Gmail accounts

Direct voter participation impact

Further reconciliation required

Description of incident

In addition to the challenges experienced with the bulk email delivery infrastructure, the technical team received reports that some students using personal Gmail accounts were unable to receive their OTP verification emails.

This was an important development because the authentication difficulties were not limited to students using institutional email addresses.

Some students had valid Gmail accounts and were able to access the internet and the X-HAT website, but did not receive the required OTPs to complete authentication.

Since OTP verification was a mandatory requirement before students could access the ballot, the inability to receive the verification code prevented the affected students from proceeding with voting.

Nature of the problem

The reported issue involved the delivery of authentication emails to Gmail users.

Potential contributing factors requiring further investigation include:

- Email provider sending restrictions.
- Gmail spam and security filtering.
- Sender-domain authentication and reputation.

- SPF, DKIM and DMARC configuration.
- Email delivery deferrals or bounces.
- High-volume email sending patterns.
- Temporary restrictions imposed by email service providers.

It is important to distinguish between emails that were successfully accepted by the sending service and emails that were actually delivered to recipients' inboxes.

A successful email sending request does not necessarily mean that the student received the OTP.

The exact technical reason for each Gmail delivery failure should therefore be established through available delivery logs and DNS authentication records.

Impact on the voting process

This incident had a direct impact on voter participation.

The affected students could not complete the mandatory authentication process and, consequently, were unable to access the electronic ballot and cast their votes.

The implications included:

1. Eligible students being unable to exercise their right to participate.
2. Students experiencing repeated attempts to request OTP verification codes.
3. Delays and frustration during the authentication process.
4. Potential abandonment of the voting process by students who could not receive their verification codes.
5. Possible underrepresentation of eligible students in the final voter turnout.

This is particularly important because a student could have valid identification information, be recognised in the university database and have a working internet connection, but still be prevented from voting because the OTP was not delivered.

Accountability consideration

The number of students affected by Gmail OTP delivery failures has not yet been quantified.

It is therefore recommended that the technical team reconcile the OTP generation records, sending logs, delivery reports and student queries to establish the extent of the problem.

For future elections, email delivery should be tested across institutional and personal email providers before the voting process begins.

5. CONSOLIDATED INCIDENT AND DOWNTIME REGISTER

The following table provides a summary of the reported incidents and their approximate durations.

No.	Incident	Approximate duration	Primary impact
1	Application/database time discrepancy	20 minutes	Delayed commencement
2	University Wi-Fi accessibility	30 minutes	Students on university Wi-Fi unable to access the domain
3	Original Mailchimp suspension	Not established	OTP delivery disruption
4	Replacement Mailchimp account transition	45 minutes	OTP delivery interruption
5	University SMTP integration	No separate duration established	Alternative delivery channel unavailable
6	DNS propagation and email restoration	30 minutes	Delayed restoration of email configuration
7	Gmail OTP delivery failures	Not established	Some eligible students unable to authenticate and vote

5.1 Understanding the different categories of downtime

For purposes of accurate reporting, the incidents should be separated into three categories.

A. Website accessibility interruptions

These are periods when students could not access the voting website.

The identified incidents were:

- 20-minute delay at the beginning of voting.
- Approximately 30-minute university Wi-Fi accessibility issue.

The Wi-Fi incident was network-specific. Students using mobile data could still access the platform.

B. Authentication and OTP delivery interruptions

These are periods when students could not reliably receive the OTPs required to access the ballot.

These included:

- Suspension of the original Mailchimp account.
- Transition to the replacement account.
- Trial account restrictions.
- Limited cPanel email capacity.
- Unsuccessful SMTP integration.
- DNS propagation and restoration.
- Reported OTP delivery failures affecting Gmail users.

C. Cumulative identified disruption periods

Combined reported durations

125 minutes

2 hours and 5 minutes

This figure adds the four reported durations: 20 + 30 + 45 + 30 minutes.

It does not include the unquantified Mailchimp suspension, SMTP investigation or Gmail delivery failures.

Important qualification: The 125 minutes represent the sum of reported incident windows, not verified continuous platform-wide downtime. Some incidents affected only specific services or categories of users, and there may have been overlap between the email-related interruptions.

It would therefore be inaccurate to state that the entire X-HAT platform was offline for 2 hours and 5 minutes.

A definitive downtime assessment requires timestamped application logs, database records, email delivery reports and network monitoring evidence.

6. IMPACT ON THE VOTING PROCESS

The incidents experienced during the election had operational implications beyond the technical availability of the website.

The most significant impact was the interruption of students' ability to complete the full voting process.

6.1 Delayed commencement

The initial time synchronisation issue prevented the platform from accepting votes at the intended opening time.

The approximately 20-minute delay affected the planned commencement of the election.

6.2 Unequal network accessibility

The university Wi-Fi issue temporarily affected students relying on campus connectivity.

Students using mobile data could continue accessing the website, while those relying on university Wi-Fi encountered difficulties.

This introduced unequal access conditions during the affected period.

6.3 OTP delivery interruptions

The suspension of Mailchimp and subsequent email service transitions disrupted the authentication process.

Students could access the website but could not necessarily complete authentication if their OTPs were not delivered.

This distinction is important because website accessibility alone does not establish that a student could successfully participate in voting.

6.4 Students unable to vote due to Gmail OTP failures

The reported Gmail delivery failures represent a particularly significant impact.

Some students were unable to receive their verification codes despite having valid Gmail accounts and being otherwise eligible to vote.

Because the OTP was a mandatory authentication requirement, these students could not proceed to the ballot.

This means the voting exercise experienced cases where eligible students were prevented from participating due to authentication delivery challenges.

The number of affected students must still be established through a reconciliation exercise.

6.5 Increased student support requirements

The incidents also increased the need for technical assistance.

Students experiencing access and authentication difficulties required guidance, troubleshooting and clarification.

The technical team had to manage these concerns while simultaneously investigating infrastructure issues and communicating with the university's ICT Department and external service providers.

6.6 Potential effect on voter turnout

The combined incidents may have affected the overall participation rate.

Students who could not access the platform or receive OTPs may have:

- Delayed their participation.
- Made repeated attempts to authenticate.
- Abandoned the voting process.
- Been unable to vote before the official closing time.

Consequently, the final voter turnout may not fully reflect the number of eligible students who intended to participate.

However, the extent of this impact cannot be quantified without analysing the number of affected students, failed OTP requests, incomplete authentication sessions and successful voting transactions.

7. IMPACT ON THE OVERALL ELECTION RESULTS AND DATA INTEGRITY

The technical incidents must be considered in two separate contexts:

1. The accessibility and participation of eligible students.
2. The integrity and accuracy of votes successfully recorded by the platform.

These are related but separate considerations.

7.1 Potential impact on voter turnout

The inability of some students to access the website or receive OTPs may have affected the number of students who successfully participated in the election.

In particular, the Gmail OTP delivery failures demonstrate that some eligible students could not complete the authentication process.

This raises an important consideration when interpreting the final voter turnout.

A student who was eligible to vote but could not receive an OTP should not automatically be considered a student who chose not to participate.

The distinction between voluntary non-participation and technical inability to participate should be recognised in the post-election assessment.

7.2 Potential impact on the election outcome

The incidents do not automatically establish that the votes successfully recorded by X-HAT were compromised or incorrectly counted.

However, they raise a legitimate question regarding whether all eligible students had a reasonable opportunity to participate.

The inability of some students to vote could potentially affect the overall participation figures and, depending on the number of affected students and the distribution of their voting preferences, could have implications for electoral outcomes.

It would be inappropriate to speculate about how the results might have changed.

A technical report can establish the availability and integrity of recorded votes, but cannot independently determine what the affected students would have voted for.

7.3 Database and voting transaction integrity

The X-HAT platform incorporated student verification and voting-status functionality.

These controls were intended to:

- Verify students against the institutional database.
- Restrict access to eligible students.
- Record successful voting submissions.
- Update voting status after successful submission.
- Prevent students from voting more than once.

Nevertheless, a formal post-election reconciliation is recommended to verify that these controls operated as intended throughout the election.

The following checks should be performed:

Verification area	**Required assessment**
Student eligibility	Confirm that participating students matched the authorised university database.
Successful votes	Confirm that every counted vote has a corresponding committed database transaction.
Duplicate submissions	Check for duplicate voting transactions.
Voting status	Reconcile students marked as having voted against successful voting records.

Failed submissions	Identify incomplete or unsuccessful voting attempts.
Voting period	Confirm that votes were recorded within the authorised election window.
Database integrity	Review database errors, interruptions and transaction failures.
Administrative access	Review administrative activity and any changes to voting records.
Results	Reconcile the final results against the underlying voting transactions.

Particular attention should be given to students who may have attempted authentication multiple times. Multiple OTP requests should not be confused with multiple votes, and an interrupted submission should be checked to establish whether it was successfully committed before another attempt was made.

7.4 Protection of the election results

The final election results should be generated from successfully recorded voting transactions rather than email delivery records, OTP requests or website traffic.

If the reconciliation confirms that votes were correctly recorded, duplicate submissions were prevented and the results were generated from the correct database records, this would provide a technical basis for confirming the integrity of the recorded results.

However, the separate issue of eligible students who could not vote must remain part of the overall electoral assessment.

8. CORRECTIVE ACTIONS IMPLEMENTED BY SM SOLUTIONS

Throughout the voting exercise, SM Solutions PE Trading (Pty) Ltd undertook several interventions to restore the affected services.

The following table summarises the actions undertaken.

Technical challenge	**Corrective action**
Application and database time discrepancy	Corrected time settings and tested voting functionality.
University Wi-Fi accessibility	Escalated the issue to UFH ICT and conducted alternative connectivity testing.
Original Mailchimp suspension	Submitted a formal appeal to the service provider.

OTP delivery interruption	Reverted to the existing cPanel email infrastructure.
Limited cPanel sending capacity	Initiated migration to a replacement Mailchimp account.
Replacement account restrictions	Investigated paid subscription activation and alternative delivery arrangements.
University SMTP connection failure	Engaged UFH ICT to investigate institutional SMTP connectivity.
DNS propagation	Monitored configuration changes until propagation was completed.
Gmail OTP delivery complaints	Identified the need for further email delivery and authentication investigation.
Final service restoration	Continued monitoring the application and email functionality until voting closure.

These interventions required the technical team to manage several interconnected services simultaneously while the election was in progress.

The team remained engaged in restoring the affected functionality and maintaining the availability of the voting platform.

9. LESSONS LEARNT AND TECHNICAL RECOMMENDATIONS

The voting exercise highlighted several areas requiring improvement before future university-wide elections.

The most important lesson is that a digital voting platform must be designed not only to accommodate high website traffic but also to sustain the entire authentication and voting process when individual service providers or network components experience disruptions.

9.1 Dedicated transactional email infrastructure

The reliance on a single external email delivery provider exposed the voting process to third-party service restrictions.

Mailchimp is primarily a marketing automation and bulk communication platform. Although it can be used for email campaigns, a high-volume OTP authentication environment requires infrastructure specifically configured for transactional messaging.

SM Solutions recommends implementing a dedicated transactional email service.

Potential providers include:

- Amazon Simple Email Service (SES).
- Brevo.
- Twilio SendGrid.
- Microsoft Azure Communication Services.

The selected provider should be configured, verified and load-tested before the commencement of voting.

9.2 Secondary email delivery and failover

A backup email provider should be configured before the election.

The system should be capable of switching to an alternative provider when the primary service experiences an outage or sending restriction.

Recommended implementation:

- Primary transactional email provider.
- Secondary transactional email provider.
- Independent sender-domain verification.
- Pre-approved sending capacity.
- Automated delivery monitoring.
- Controlled failover.
- Email delivery and failure reporting.

This would reduce the risk of an entire authentication process depending on one external service.

9.3 Gmail and other external email provider testing

Future elections should incorporate email delivery testing across different email providers.

Testing should include:

- Institutional university email addresses.
- Gmail.
- Outlook and Hotmail.
- Other commonly used personal email providers.

The technical team should verify actual receipt of OTPs rather than simply confirming that an email was accepted by the sending service.

SPF, DKIM and DMARC records should also be configured correctly to improve sender authentication and email deliverability.

9.4 Alternative authentication mechanisms

Given the challenges experienced with OTP email delivery, alternative authentication arrangements should be explored.

Possible options include:

- University Single Sign-On (SSO), if supported by UFH.
- An approved SMS OTP service.
- Institutional identity verification.
- Secure alternative verification mechanisms approved by the university.

Any alternative should retain strong identity verification, prevent duplicate voting and protect the confidentiality of the electoral process.

9.5 Server capacity and load testing

The platform should undergo load and stress testing before future elections.

The testing should simulate the anticipated student population accessing the system simultaneously.

Recommended measures include:

- Concurrent-user testing.
- Database performance optimisation.
- Server CPU and memory monitoring.
- Database connection optimisation.
- Application response-time monitoring.
- Rate limiting.
- Traffic management.
- Capacity scaling.
- Backup and recovery testing.

9.6 University network integration

The university should facilitate formal network compatibility testing before voting commences.

The following should be verified:

- X-HAT domain accessibility.
- DNS resolution.
- Firewall and web-filtering permissions.
- HTTPS connectivity.
- Network capacity.
- SMTP connectivity, where applicable.

A formal confirmation from UFH ICT should be obtained before the election opens.

9.7 Time synchronisation

All relevant environments should use consistent and synchronised time sources.

The technical team should implement:

- Automated NTP synchronisation.
- Consistent timezone configuration.
- Application and database timestamp verification.
- Automated opening and closing time tests.
- Pre-election validation.

UTC should preferably be used internally for system timestamps, with South African Standard Time (SAST) applied for election administration and reporting.

9.8 Centralised monitoring and incident management

Future deployments should incorporate a centralised monitoring solution.

This should provide visibility into:

Monitoring area	Information required
Website	Availability and response time
Server	CPU, memory and storage utilisation
Database	Connections, errors and transaction performance

Email	OTP generation, sending, delivery and failure rates
DNS	Domain resolution and configuration
Security	Authentication attempts and suspicious activity
Voting	Successful submissions and failed transactions

An incident register should record the detection time, acknowledgement time, investigation, root cause, corrective action and restoration time of every incident.

10. PROPOSED FUTURE ELECTION READINESS FRAMEWORK

SM Solutions recommends that the university and technical team jointly implement a formal election-readiness framework.

This will ensure that technical infrastructure, institutional networks and third-party services are tested before the next voting exercise.

Area	Recommended intervention	Priority
Hosting	Capacity assessment and load testing	Critical
Database	Transaction integrity and backup verification	Critical
Email	Dedicated transactional email provider	Critical
Email redundancy	Fully configured secondary email service	Critical
Authentication	OTP delivery and alternative authentication testing	Critical
University network	Domain whitelisting and connectivity testing	Critical
Time settings	NTP and timezone synchronisation	High
Security	Vulnerability assessment and security testing	High
Monitoring	Real-time infrastructure monitoring	High
Disaster recovery	Documented recovery and failover procedures	High
Reporting	Automated election activity and audit reporting	High
Student support	Dedicated election support and query management	High

10.1 Recommended pre-election testing schedule

Period	Activity

7 days before voting	Infrastructure assessment, email provider verification and security checks
72 hours before voting	Load testing and institutional network compatibility testing
48 hours before voting	Full authentication and OTP delivery testing across email providers
24 hours before voting	Final system checks and database backup verification
Before opening	Confirm server time, voting configuration and email service capacity
During voting	Continuous monitoring of website, database, email and network performance
After closure	Secure database backup, audit review and voting transaction reconciliation

A formal technical readiness sign-off should be completed by SM Solutions and the designated university ICT representative.

11. OVERALL TECHNICAL ASSESSMENT AND ACCOUNTABILITY

Based on the reported incidents, the X-HAT voting exercise experienced disruptions across three primary technical areas:

1. Application configuration: The initial discrepancy between application and database time settings delayed the opening of voting by approximately 20 minutes.

2. Network accessibility: The university Wi-Fi incident temporarily prevented students relying on campus connectivity from accessing the voting domain. This was escalated to UFH ICT and resolved after approximately 30 minutes.

3. Authentication and email infrastructure: The suspension of the original Mailchimp account, restrictions on the replacement account, limited cPanel sending capacity, unsuccessful SMTP integration and DNS propagation challenges disrupted OTP delivery.

The Gmail OTP delivery complaints further demonstrated that the authentication challenges had a direct impact on some students' ability to participate.

11.1 Assessment of system availability

It is important to clarify that the X-HAT website, database and email authentication infrastructure were separate components.

Not every incident resulted in the entire website becoming unavailable.

For example:

- During the university Wi-Fi incident, mobile data users could still access the website.
- During the Mailchimp suspension, the primary disruption concerned email authentication.
- During the replacement account transition, email delivery was affected by provider restrictions.
- Gmail users who did not receive OTPs could not complete authentication, even where the website itself was accessible.

Therefore, the incidents should be classified as a combination of website accessibility interruptions and authentication service disruptions, rather than one continuous platform outage.

11.2 Assessment of the technical team's response

The technical team undertook active intervention throughout the voting exercise.

This included:

- Investigating and correcting application configuration.
- Testing accessibility through alternative networks.
- Engaging UFH ICT.
- Submitting a Mailchimp suspension appeal.
- Implementing alternative email delivery arrangements.
- Attempting institutional SMTP integration.
- Monitoring DNS propagation.
- Communicating with external service-provider support.
- Restoring email functionality.
- Monitoring the platform until voting closure.

Following the final restoration, no further technical glitches were reported until voting was officially closed.

11.3 Areas requiring further verification

Although the affected services were restored, certain matters require additional evidence before a definitive assessment of the overall election can be made.

These include:

1. The exact number of students affected by OTP delivery failures.
2. The number of Gmail users who did not receive their verification codes.
3. The number of OTPs successfully delivered, bounced or deferred.
4. The number of students who attempted authentication but did not complete it.
5. The total number of successfully recorded votes.
6. The number of students marked as having voted.
7. Whether any voting transactions failed or were interrupted.
8. Whether any votes were recorded outside the authorised voting period.

These checks will enable the university to distinguish between students who did not participate voluntarily and those who may have been prevented from participating by technical challenges.

12. CONCLUSION AND FORMAL ACCOUNTABILITY STATEMENT

SM Solutions PE Trading (Pty) Ltd acknowledges the technical interruptions experienced during the University of Fort Hare's X-HAT digital voting exercise.

As the technical development and hosting partner, we recognise that the availability, security and reliability of the platform were fundamental to ensuring that eligible students could participate in the SRC electoral process.

The incidents experienced during the election presented significant operational challenges, particularly because the voting process was already underway when some of the external service dependencies became unavailable.

The technical team had to respond to multiple incidents involving application configuration, university network accessibility and third-party email delivery services.

We acknowledge that the initial time synchronisation discrepancy delayed the commencement of voting, while the university Wi-Fi accessibility issue temporarily restricted access for students relying on campus connectivity.

We further acknowledge that the suspension of the original Mailchimp account created the most significant operational challenge, as the email authentication service was essential to enabling students to access the ballot.

The subsequent transition to a replacement account, trial sending restrictions, limited cPanel capacity, unsuccessful SMTP integration and DNS propagation delays prolonged the authentication challenges.

Of particular concern were the students using personal Gmail accounts who were unable to receive their OTP verification codes and were consequently unable to complete authentication and cast their votes.

We acknowledge that these students were affected beyond a mere inconvenience: the failure to receive their authentication codes prevented them from participating in the voting process.

This is a material consideration when assessing the accessibility and overall participation levels of the election.

Despite the challenges, SM Solutions remained actively engaged in investigating and resolving the incidents. Alternative delivery arrangements were implemented, the university ICT team was engaged, and communication with the relevant service providers continued until the affected services were restored.

Following restoration, the platform operated without further reported technical glitches until voting was officially closed.

We nevertheless recognise that restoring system functionality does not, on its own, establish that every eligible student had an equal opportunity to participate or that the final voter turnout was unaffected.

For this reason, we recommend a joint post-election technical review involving the university, the Electoral Committee, UFH ICT and SM Solutions.

The review should establish the number of students affected by access and authentication failures, reconcile the successful voting transactions, verify the integrity of the recorded results and assess whether any further electoral considerations are necessary.

Our position is that the technical incidents must be transparently acknowledged, documented and assessed independently of the final election results.

The objective should not simply be to establish that the platform was restored, but to ensure that the electoral process is supported by infrastructure that is accessible, resilient, secure and capable of accommodating the participation requirements of the entire student population.

SM Solutions remains committed to strengthening the X-HAT platform and implementing the necessary improvements to support future digital elections.

We appreciate the cooperation of the University's ICT Department and other stakeholders who assisted in addressing the challenges encountered during the voting exercise.

13. ANNEXURES AND SUPPORTING EVIDENCE

To strengthen the credibility of this report and support its submission to University Management, the Electoral Committee and other relevant stakeholders, the following evidence should accompany the report where available.

Annexure	Supporting evidence	Purpose
A	Application server logs	Establish website availability and application errors
B	Database logs and voting transaction records	Verify database activity and recorded votes
C	Mailchimp suspension notification	Establish the external service suspension
D	Mailchimp appeal correspondence	Demonstrate attempts to restore the original account
E	cPanel email delivery reports	Establish email sending volumes and limitations
F	Replacement Mailchimp account records	Confirm trial restrictions and activation issues
G	DNS configuration and lookup records	Support the DNS propagation timeline
H	UFH ICT correspondence	Document university Wi-Fi escalation and resolution
I	SMTP integration correspondence	Document the attempted university email integration
J	OTP delivery and failure reports	Establish authentication delivery performance
K	Student query records	Identify students who reported access or OTP problems

L	Voting status reconciliation	Establish the number of students marked as having voted
M	Final voting transaction report	Verify the number of successfully recorded votes
N	Administrative audit logs	Establish administrative actions and changes

14. FINAL DECLARATION

We confirm that this report has been prepared to provide an account of the technical incidents experienced during the X-HAT Digital Voting exercise, the corrective measures undertaken and the potential implications for student participation.

The report is based on the incidents and operational information available to the technical team at the time of preparation.

The exact number of affected students, final downtime calculations and the integrity of the recorded results remain subject to verification against the relevant technical logs and voting records.