ADVISORY ON ONLINE CAMPAIGNING AND CYBERSECURITY PROTOCOLS

As the upcoming 2020 General Elections (GE2020) will be held amidst safe-distancing measures due to COVID-19, physical campaigning activities will be heavily restricted. Election rallies will be disallowed, while walkabouts and door-to-door campaigning will be subject to safe distancing measures, thus limiting the scale of such activities.

2 In the absence of these traditional methods of campaigning, there will be a shift towards the broadcast and Internet medium for campaigning and outreach purposes. To support political parties and candidates with this shift, the Government is making arrangements to provide recording venues for "e-rallies".

3 This advisory aims to provide political parties and candidates with guidelines on online campaigning, and cybersecurity protocols that one should observe for the purpose of live streaming activities on the Internet.

1 Online Campaigning

1.1 Political parties and candidates may carry out campaigning activities on the Internet, including live streaming, throughout the election period. Their campaigning activities online are subject to prevailing laws. The display of election advertising, which will include livestreams or recorded livestreams, by the political parties and candidates must abide by the Parliamentary Elections Act and the Parliamentary Elections (Election Advertising) Regulations.

1.2 Films that are only posted online need not be submitted to the Infocomm Media Development Authority (IMDA) for film classification, but the content should comply with the Internet Code of Practice (ICOP).

1.3 Candidates and voters must not make, exhibit or distribute party political films (PPFs). PPFs include films that are made by any person and directed towards any political end in Singapore, such as those intended or likely to affect voting in any election in Singapore. Factual and objective films that do not dramatise and/or present an inaccurate account, such as live recordings of events held in accordance with the law, factual documentaries, manifestos of the political party, or the candidate's declaration of policies, will not be considered PPFs. For example, a recording of a livestream of an online rally that is not modified to present an inaccurate account is allowed. However, a recording of a livestream that employs dramatisation and/or animation to present an inaccurate account, sensationalise and mislead viewers on political matters is likely to be considered a party political film.

1.4 Political parties, candidates and their authorised representatives should conduct election campaigning in a responsible and dignified manner that befits the seriousness of the election process. They should steer away from negative campaigning practices based on hate and denigration of opposing candidates. They should not make false statements that allege corruption or commission of criminal offences, or statements that may cause racial or religious tensions or affect social cohesion.

1.5 The outcome of Singapore elections is for Singaporeans to decide. As such, candidates should ensure that their election campaign is free from foreign influence. Only Singapore Citizens can take part in election activities and campaigning. Any Singapore Citizen who wants to conduct any election activity (whether online, offline or both) for a candidate must first be in possession of a written authority signed by a candidate or his election agent in Form 22 or Form 23 of the First Schedule of the Parliamentary Elections Act.

1.6 A cooling-off period where all campaigning must stop will be observed from midnight on Cooling-off Day and until after polls close on Polling Day, unless otherwise exempted.

2 Cybersecurity

2.1 As part of the preparations for the live streaming of the e-rallies, political parties and candidates are responsible to get their own Information Technology (IT) infrastructure[1] and online platforms[2] ready for broadcast. Political parties and candidates should also take appropriate measures to secure such infrastructure and

[1] As described in the Advisory to Political Parties on Cybersecurity Risks and Precautionary Measures, IT infrastructure includes any smartphone, computer and computing device, online and social media assets, as well as data storage and management.

[2] Online platforms refers to the channels that political parties choose to use for their live streaming of the e-rally. These can include the party's or candidate's website, social media platforms (e.g. Facebook, Instagram, YouTube etc.) and web conferencing platforms (e.g. Cisco WebEx, Microsoft Teams, Zoom, etc.).

online platform accounts against unauthorised access, modification or deletion. This will ensure a smooth and uninterrupted streaming of the e-rally during the balloted timeslots.

2.2 This advisory provides information on possible cybersecurity related incidents that could cause disruption to the live streaming, and precautionary measures that political parties and candidates can take to secure their IT infrastructure and online platforms. It should be read in conjunction with the Advisory to Political Parties on Cybersecurity Risks and Precautionary Measures.

2.3 Because political parties and candidates use various IT infrastructure and online platforms to support the live streaming of the e-rally, accessibility to online platforms to live-stream the e-rally could be affected if devices such as network routers or computers get compromised. Broadcast of the e-rally on the online platform(s) could be disrupted if the account(s) is not secured and parties or candidates get locked out of their account(s). Websites that are not updated could be prone to defacement attacks. Website availability could become an issue if websites are not sized to handle the increased traffic volume during the broadcast, or if the website suffers a denial of service attack.

2.4 Precautionary measures that the political parties can take include, but are not limited to:

i. IT Infrastructure

- Control or restrict administrator and remote access privileges
- Keep devices' software updated
- Install anti-virus software and firewalls
- Monitor the devices and network to detect any breaches or unusual activities
- Enable security logging, if available
- Back up important and sensitive data
- Staff are to be vigilant for phishing emails or text messages

ii. Political Parties' Websites

- Update the website to address known security vulnerabilities
- Increase the bandwidth to your website to accommodate large traffic network, and ensure that the network is adequate to meet your streaming needs
- Consider subscribing to a distributed denial of service mitigation solution from your Content Delivery Network provider
- Implement traffic monitoring to receive advanced notice of overloading

- Enable log auditing to capture any suspicious activities

iii. Online Platforms

- Only download applications from the official Play Store (Android) and App Store (iOS)
- Use strong passwords, and two-factor authentication for devices and social media accounts where possible
- Be vigilant for phishing emails or text messages
- Monitor for unusual activities in your devices or accounts

2.5 Political parties and candidates are responsible for their own cybersecurity. They should appoint someone to take charge of their cybersecurity matters and engage a professional vendor to review and manage the cybersecurity posture for their party, and to deal with an incident, as and when it happens. They can refer to the Advisory to Political Parties on Cybersecurity Risks and Precautionary Measures for a list of email and social media providers if they have issues with their email or social media accounts. The advisory also contains a non-exhaustive list of cybersecurity vendors that they can consider to appoint, to review and manage the cybersecurity posture of their party, as well as to deal with any cybersecurity incident in the lead-up and live-stream of the e-rally.

3 Connectivity and Streaming Platforms

3.1 Political parties and candidates are recommended to consider the following when preparing for their own, self-conducted livestreams:

Adequacy and resiliency of Internet connection

3.2 **Adequacy of Internet capacity and bandwidth at self-sourced venue.** Political parties and candidates should assess the required Internet bandwidth necessary to support their live streaming and procure the appropriate connectivity offering.

3.2.1 **Resilience of Internet connection at self-sourced venue.** When sourcing for venues for live streaming, political parties and candidates may wish to consider venues that have alternate or backup Internet connections, and/or continuity plans in place if the connection is disrupted.

Suitability of platforms (e.g., YouTube and Facebook Live) for live streaming

3.3 **Technical suitability of platforms.** Political parties and candidates should select reliable streaming platforms that have sufficient and adequate network capacity and bandwidth to cater to the expected number of concurrent viewers viewing their livestreams.

Live streaming best practices

3.4 **Chat and viewing moderation**. Political parties and candidates may wish to review the entry settings for their live streaming sessions if the platform enables them to do so, to verify attendees and prevent unwanted disruptions. They should also moderate the on-going chat sessions, if their live streaming platform has a chat function. This would help to better ensure healthy engagement during the live streaming.

3.5 **Contingency messaging in the event of technical issues**. Political parties and candidates may wish to prepare a platform or channel to communicate with and provide updates to viewers in the event that technical issues disrupt their livestream.

MINISTRY OF COMMUNICATIONS AND INFORMATION

ELECTIONS DEPARTMENT

24 JUNE 2020