# Peningkatan Keterampilan Keamanan Siber bagi Pengelola Situs Desa Baros Kabupaten Serang

**Jati Satrio*[1], Siti Maryam[2], Aniqotul Ummah[3], Danis Tri Saputra Wahidin[4]**

[1]Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
[2]Ilmu Komunikasi, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
[3,4]Ilmu Politik, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
*e-mail: jatisatrio@upnvj.ac.id[1], sitimaryam@upnvj.ac.id[2], aniqotulummah@upnvj.ac.id[3], daniswahidin@upnvj.ac.id[4]

***Abstrak***

*Perkembangan teknologi informasi dan komunikasi membuat berbagai elemen masyarakat, termasuk desa, mengembangkan situs dan media sosial. Namun, sering kali pengelola situs dan media sosial abai terhadap aspek keamanan siber. Keamanan siber menjadi aspek penting dalam menjaga informasi, data, dan jaringan yang dimiliki suatu situs dan media sosial. Pelatihan peningkatan keterampilan keamanan siber menjadi solusi yang digagas untuk memberikan pemahaman dasar kepada pengelola situs dan media sosial Desa Baros. Metode yang dipilih berupa pelatihan kemampuan dasar keamanan siber yang diisi dengan ceramah, diskusi, dan praktik terkait dengan keamanan siber. Pelatihan dilakukan secara tatap muka dan terpusat agar peserta dapat betul-betul memahami permasalahan keamanan siber dalam pengelolaan situs desa dan media sosial desa. Pelatihan peningkatan keterampilan keamanan siber berhasil memberikan pemahaman dasar terkait keamanan siber kepada pengelola situs dan media sosial Desa Baros. Pelatihan peningkatan keterampilan keamanan siber ini berhasil memberikan pemahaman dan kemampuan dasar bagi para peserta dalam membangun keamanan siber yang diperlukan bagi situs dan media sosial Desa Baros.*

***Kata kunci**: Keamanan Siber, Media Sosial, Website Desa*

***Abstract***

*Information and communication technology development has made various elements of society, including villages, develop websites and social media. However, often site and social media managers ignore the cybersecurity aspect. Cyber security is essential in maintaining information, data, and networks owned by a site and social media. Cybersecurity skills training is a solution that was initiated to provide a basic understanding to the site managers and social media of Baros Village. The chosen method is basic cyber security skills training filled with lectures, discussions, and practices related to cyber security. The training is conducted face-to-face and centrally so that participants can genuinely understand cybersecurity issues in managing village sites and social media. The cybersecurity skill improvement training has provided a basic understanding of cybersecurity to the site managers and social media of Baros Village. The cybersecurity skill improvement training succeeded in providing participants with a basic understanding and skills in building the necessary cyber security for the Baros Village website and social media.*

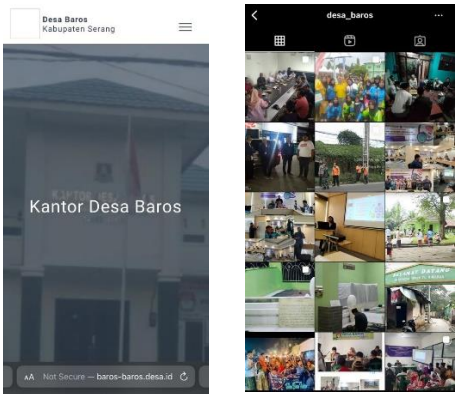
***Keywords**: Cybersecurity, Social Media, Village Website*

## 1. PENDAHULUAN

Pengaplikasian teknologi digital dan internet dalam pengembangan pelayanan terhadap masyarakat perlu diimbangi dengan menumbuhkan pemahaman mengenai keamanan siber. Apabila digitalisasi tidak diimbangi dengan sistem keamanan siber yang kuat, maka dikhawatirkan akan tercipta kerentanan dalam sistem yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Pada saat pihak tersebut dapat menerobos sistem keamanan digital yang dibangun oleh suatu institusi maka akan timbul kerusakan dan kerugian terhadap kehidupan bermasyarakat.

Dewasa ini, penerapan teknologi digital juga menjadi sebuah keniscayaan di tingkat desa. Desa-desa di seluruh Indonesia berlomba-lomba untuk masuk ke arena digital dengan membangun situs desanya masing-masing. Situs desa adalah laman virtual satu desa yang resmi disediakan oleh pemerintah dengan menggunakan domain berakhiran .desa.id. Keberadaan website desa ini sejalan dengan target pemerintah untuk melakukan transformasi digital hingga elemen paling kecil dalam pemerintahan, yaitu desa (Saefudin, 2022). Transformasi digital di tingkat desa saat ini masih berjalan dengan tingkat yang beragam. Beberapa desa sudah mengimplementasikan berbagai teknologi baru seperti *access point* internet, CCTV, dan tombol darurat kesehatan dan keamanan untuk menunjang kinerja desa, namun masih banyak desa yang belum mengadopsi teknologi baru tersebut mengingat banyak proses di desa tersebut masih dilakukan secara analog (Nurchim & Nofikasari, 2018).

Mitra pengabdian dalam artikel ini adalah Desa Baros. Desa Baros baru saja membangun sebuah situs desa dengan alamat http://baros-baros.desa.id dan profil Instagram dengan nama pengguna @Desa_Baros. Walau pun Desa Baros telah memiliki sebuah situs desa, tetapi pemahaman pengelola situs dan media sosial Desa Baros masih belum maksimal terkait dengan keamanan siber. Tim pengabdi mengadakan pengabdian dengan tujuan untuk memberikan pemahaman dasar terkait dengan keamanan siber kepada pengelola situs desa dan media sosial pemerintah desa di Desa Baros. Gambar 1 menunjukkan tampilan muka dari situs desa milik Desa Baros dan laman profil Instagram Desa Baros.




(a) (b)

Gambar 1. Profil digital Desa Baros (a) situs baros-baros.desa.id dan (b) Instagram @Desa_Baros

Keamanan siber menjadi sangat penting ketika dikaitkan dengan tren kejahatan siber yang tengah meningkat di masyarakat dewasa ini. Keamanan data pribadi dan institusi, bahkan bagi generasi muda yang cenderung mahir menggunakan teknologi, masih sangat rentan untuk bocor dan dimanfaatkan oleh pihak yang tidak bertanggung jawab yang dapat memanfaatkan kelengahan sistem keamanan siber (Revilia & Irwansyah, 2020). Semakin maraknya kejahatan siber berbanding lurus dengan semakin terintegrasinya teknologi informasi dan komunikasi dalam kehidupan bermasyarakat di Indonesia, termasuk di desa sebagai elemen terkecil masyarakat. Pemerintah Indonesia pun menaruh perhatian ekstra terhadap permasalahan keamanan siber dimana pemerintah membentuk Badan Siber dan Sandi Negara (BSSN) untuk menjaga keamanan dan kedaulatan siber, dan Pemerintah Indonesia juga aktif berperan mendorong isu kemanan siber di tingkat bilateral dan multilateral (Chotimah, 2019).

Tim pengabdi melihat bahwa permasalahan keamanan siber dapat menjadi satu hal yang penting dan perlu diperhatikan dengan sangat teliti. Penelitian menunjukkan bahwa kewaspadaan masyarakat terhadap permasalahan keamanan siber masih cukup rendah terutama apabila kesiapsiagaan terhadap ancaman siber dianggap masih cukup rendah (Nam, 2019). Mengingat pentingnya permasalahan keamanan siber dalam rangka digitalisasi, tim pengabdi merasa perlu untuk meningkatkan pemahaman masyarakat terkait dengan resiko, ancaman, dan langkah yang dapat diambil terkait dengan keamanan siber.

## 2. METODE

Proses pengabdian kepada masyarakat yang dilakukan di Desa Baros merupakan rangkaian kegiatan yang masuk ke dalam program pembangunan desa digital. Program ini merupakan program jangka panjang yang akan berjalan selama tiga tahun (2022-2024). Pada tahun pertama, tim pengabdi memiliki target untuk memberikan fondasi awal dalam pembangunan desa digital. Rangkaian kegiatan pengabdian dapat dilihat dalam Gambar 2 yang berupa diskusi kelompok terarah untuk mengetahui aspirasi elemen masyarakat desa terkait dengan digitalisasi desa, pendampingan pembuatan situs desa, dan pelatihan keahlian dasar dalam mengelola situs dan media sosial desa.

Gambar 2. Suasana diskusi kelompok terarah di Desa Baros

Dalam proses pelatihan keahlian dasar dalam pengelolaan situs dan media sosial desa terdapat beberapa materi yang diberikan, seperti fotografi, videografi, penulisan konten, dan keamanan siber. Untuk memberikan materi yang sangat padat tersebut, tim pengabdi mengundang empat orang perwakilan desa yang terdiri dari dua orang perangkat desa dan dua orang perwakilan dari karang taruna. Gambar 3 menunjukkan empat orang peserta pelatihan yang terdiri dari dua orang perangkat desa dan dua orang perwakilan karang taruna Desa Baros. Kami melakukan pelatihan secara terpadu selama tiga hari. Metode ini dipilih berdasarkan pertimbangan untuk menjaga fokus peserta selama pelatihan.


Gambar 3. Peserta pelatihan peningkatan keterampilan keamanan siber

Dalam memberikan pelatihan keamanan siber, metode yang dipilih adalah ceramah dan diskusi. Peserta pelatihan mendengarkan paparan yang disampaikan oleh pemateri dan mendiskusikan permasalahan-permasalahan yang dihadapi peserta terkait dengan keamanan siber. Lebih jauh, pemateri juga memberikan beberapa contoh metode yang dapat digunakan oleh peserta untuk memperkuat sistem keamanan siber yang dibangun pada situs dan media sosial desa.

Sesi ceramah dan diskusi yang dilakukan dibagi menjadi tiga tahapan. Pertama, peserta diberikan pemahaman mengenai konsep dan terminologi yang umum digunakan dalam ranah keamanan siber. Pengenalan konsep dan terminologi menjadi aspek penting mengingat keamanan siber merupakan wilayah kajian baru dimana belum semua elemen masyarakat

memahami konsep yang sering digunakan. Selanjutnya, tim pengabdi memberikan materi mengenai metode dan solusi sederhana apa saja yang bisa digunakan untuk memperkuat lapisan keamanan siber yang dimiliki oleh individu atau instasi. Sesi ditutup dengan melakukan diskusi mengenai pengalaman atau pertanyaan yang dimiliki oleh para peserta terkait dengan keamanan siber.

## 3. HASIL DAN PEMBAHASAN

Dalam pelaksanaan kegiatan pengabdian, tim pengabdi memberikan penjelasan mengenai konsep-konsep yang cukup sering ditemui dalam kajian kemanan siber. Konsep-konsep ini menjadi cukup rumit dikarenakan banyak yang merupakan istilah teknis dan menggunakan bahasa asing. Tim pengabdi menjelaskan konsep-konsep seperti peretasan, kejahatan siber, virus, dan malware. Gambar 4 menunjukkan suasana pelatihan peningkatan kemampuan keamanan siber yang diberikan kepada para pengelola situs desa dan media sosial Desa Baros.


Gambar 4. Suasana pelatihan keamanan siber bagi pengelola situs dan media sosial Desa Baros

### 3.1. Penjelasan Istilah dan Konsep dalam Keamanan Siber

Peretasan didefinisikan sebagai penggunaan teknologi komputer untuk tindakan-tindakan curang seperti penipuan, invasi privasi, dan pencurian data personal atau organisasi. Peretasan dilakukan oleh peretas yang pada umumnya memiliki kemampuan pemrograman komputer dan pengetahuan tentang keamanan siber. Peretas melakukan aksinya dengan mengeksploitasi kelemahan dalam sistem komputer dan jaringan untuk mendapatkan akses.

Peretasan merupakan salah satu bentuk kejahatan siber, namun masih banyak lagi bentuk kejahatan siber yang berkembang dewasa ini. Kejahatan siber pada umumnya dilakukan dengan menggunakan perantara internet, namun terkadang kejahatan siber juga bisa dilakukan dengan perantara layanan pesan singkat. Beberapa contoh kejahatan siber yang sering muncul antara lain berupa pelanggaran privasi, pencurian identitas, mengedarkan dokumen yang dilindungi hak cipta tanpa ijin, dan pencurian uang secara elektronik.

Tim pengabdi juga memberikan penjelasn mengenai virus. Virus dapat didefinisikan sebagai satu jenis peranti lunak jahat atau *malicious software* (malware) yang dapat mereplikasi dirinya dan mengubah bagaimana program satu komputer berjalan. Virus dapat menyebar dengan berbagai cara melalui unduhan di internet, lampiran satu surat elektronik, atau melalui alat seperti flashdisk. Ketika satu komputer terinfeksi oleh virus, maka komputer tersebut akan memiliki perilaku yang tidak biasa.

Selain virus, terdapat banyak jenis malware yang dapat menghinggapi dan mengganggu kinerja komputer (Rohith & Kaur, 2021). Adware merupakan salah satu jenis malware yang bekerja dengan memunculkan secara paksa iklan di layar komputer tanpa keinginan dari pengguna komputer. Sementara itu, ransomware merupakan sebuah kategori malware yang bekerja dengan cara meminta tebusan (*ransom*) kepada pengguna jika ingin mengakses kembali dokumen yang dimiliki atau jika tidak ingin data pribadi yang dimiliki pengguna disebar di internet. Terakhir adalah spyware, spyware adalah peranti yang digunakan untuk memata-matai perilaku pengguna tanpa ijin dan pengetahuan pengguna.

### 3.2. Langkah Memperkuat Sistem Keamanan Siber

Dalam menjelaskan langkah-langkah yang dapat diambil oleh pengguna perangkat untuk memperkuat sistem keamanan siber, tim pengabdi membuat tiga kategori strategi yang bisa dikembangkan oleh perangkat desa Desa Baros. Pertama adalah strategi perubahan perilaku dalam menggunakan perangkat komputer. Kedua adalah strategi pencegahan awal yang bisa dilakukan oleh tim. Terakhir adalah penggunaan aplikasi pihak ketiga untuk memperkuat sistem keamanan siber satu perangkat komputer.

Tim pengelola situs desa yang menggunakan perangkat komputer perlu mengembangkan dan menerapkan perilaku yang dapat menjaga keamanan siber satu sistem. Tim pengabdi memberikan beberapa masukan terkait perubahan perilaku tersebut. Pertama, memisahkan penggunaan perangkat, baik itu komputer atau ponsel, antara penggunaan untuk kepentingan pekerjaan dengan penggunaan untuk kepentingan pribadi. Dengan memisahkan penggunaan perangkat ini maka kejadian-kejadian yang tidak diharapkan seperti perangkat terjangkit virus dapat diminimalisir. Kedua, tidak melakukan tindakan-tindakan yang sembrono ketika menggunakan perangkat komputer seperti, mengunjungi situs yang mencurigakan, memindahkan data tanpa sepengetahuan teman tim lainnya, dan juga memasang flashdisk atau perangkat lainnya tanpa memeriksa keamanannya terlebih dahulu. Terakhir pengelola website harus mengamankan perangkat secara fisik dan juga virtual. Secara fisik perangkat ditaruh di tempat yang aman dari ancaman seperti pencurian dan bencana alam. Sedangkan secara virtual perangkat dilengkapi dengan kata sandi yang hanya diketahui oleh beberapa orang saja.

Dalam mengembangkan strategi pencegahan tingkat awal, tim pengabdi juga memberikan beberapa saran yang dapat digunakan oleh para perangkat desa. Pertama, untuk komputer yang menjadi inventaris desa hanya pasang program-program yang memang diperlukan dan selalu usahakan menggunakan program yang asli agar terhindar dari malware yang mengancam keamanan komputer dimaksud. Selanjutnya gunakan fitur Windows System Recovery yang bisa digunakan untuk mengembalikan sistem komputer seperti keadaan pada satu tanggal atau rutin melakukan *backup* terhadap dokumen-dokumen yang ada. Strategi ini penting untuk memberikan pilihan ketika dokumen tidak bisa diakses karena satu hal atau serangan. Terakhir selalu gunakan peranti lunak dengan versi paling mutakhir hal ini untuk mencegah serangan-serangan yang disebabkan oleh malware baru yang belum dikenali peranti lunak versi lama.

Strategi terakhir yang bisa digunakan oleh perangkat desa untuk mengamankan alat dan informasi yang dimiliki oleh Desa Baros adalah dengan menggunakan berbagai aplikasi untuk mendukung keamanan siber Desa Baros. Pertama, perangkat desa bisa memasang program anti malware yang berguna untuk mendeteksi dan menghapus malware yang menjangkiti komputer. Saat ini telah banyak program anti malware yang dikembangkan berbagai pihak. Program tersebut memiliki fitur-fiturnya sendiri yang bisa digunakan sesuai dengan kebutuhan pengguna. Windows versi 10 telah memiliki Windows Defender yang cukup mumpuni sebagai pertahanan dari malware yang ada. Apabila peserta ingin menggunakan aplikasi pihak ketiga, maka tim pengabdi mengusulkan untuk menggunakan MalwareBytes untuk memperkuat lini keamanan siber yang dimiliki. Kedua, tim pengabdi memperkenalkan aplikasi yang dapat membantu pengguna perangkat untuk mengaktifkan otentikasi dua faktor. Otentikasi dua faktor adalah lapisan tambahan yang dimiliki oleh satu akun selain kata sandi yang harus dimiliki sebelum mengakses akun yang dimiliki. Saat ini telah banyak tersedia aplikasi yang memudahkan pengguna untuk mengaktifkan fitur otentikasi dua faktor. Tim pengabdi menunjukkan cara menggunakan google authenticator sebagai salah satu aplikasi yang dapat digunakan untuk mengaktifkan otentikasi dua faktor. Terakhir, tim pengabdian juga memperkenalkan aplikasi pengelola kata sandi. Aplikasi pengelola kata sandi merupakan sebuah aplikasi yang diperuntukkan untuk menyimpan kata sandi yang dimiliki sehingga pengguna tidak perlu mengingat kata sandi yang dimilki.

Tim pengabdi juga memberikan beberapa tips terkait pembuatan kata sandi yang kuat. Pertama, dalam membuat kata sandi, pengguna harus menghindari penggunaan informasi pribadi, seperti tanggal lahir, nama pasangan, atau nama keluarga, dalam kata sandi tersebut.

Kedua, dalam menyusun kata sandi, walaupun penggunaan kombinasi huruf, angka, dan karakter khusus sangat dianjurkan, tetapi kata sandi yang terdiri dari gabungan karakter tersebut rentan untuk dilupakan mengingat memori manusia memang tidak didesain untuk mengingat pola yang rumit (Yıldırım & Mackie, 2019). Terakhir, penyusunan kata sandi yang kuat adalah dengan menggunakan jumlah karakter yang banyak. Hal ini dapat disiasati dengan menyusun kata sandi yang terdiri dari gabungan dua frasa umum sehingga akan membuat kata sandi yang relatif panjang, sulit ditebak, dan mudah diingat.

### 3.3. Sesi Diskusi

Setelah tim pengabdi selesai melakukan paparan dan percontohan terkait dengan materi keamanan siber, tim pengabdi mengajak para peserta untuk berdiskusi. Diskusi dibuka dengan menanyakan sejauh mana strategi keamanan siber telah diterapkan di Desa Baros terutama terkait dengan pelayanan digital Desa Baros. Sejauh pengetahuan peserta, keamanan siber baru dilakukan sebatas memasang kata sandi di alat-alat yang dimiliki oleh Desa Baros. Komputer dan inventaris lainnya yang dimiliki oleh Desa Baros belum dilengkapi dengan fitur dan aplikasi yang dapat digunakan untuk memperkuat sistem keamanan siber.

Diskusi dilanjutkan dengan membuka sesi pertanyaan. Terdapat dua pertanyaan yang muncul dari peserta. Pertanyaan pertama datang dari perangkat Desa Baros. Peserta menanyakan mengenai metode yang dapat dilakukan untuk mendapatkan peranti lunak asli untuk aplikasi-aplikasi yang memang sangat esensial untuk kegiatan pemerintahan. Peserta memahami bahwa peranti lunak asli merupakan hal yang sangat penting dalam konteks keamanan siber, namun untuk mendapatkan peranti asli tersebut, masyarakat harus mengeluarkan uang yang cukup banyak dan hal ini juga belum menjadi perhatian dalam anggaran belanja desa. Pertanyaan kedua datang dari perwakilan Karang Taruna. Perwakilan Karang Taruna bertanya mengenai langkah-langkah yang harus dilakukan ketika satu perangkat yang dimiliki diindikasi terjangkit malware.

Dalam menjawab pertanyaan pertama, tim pengabdi memahami bahwa kendala dana merupakan hambatan terbesar dalam mendapatkan peranti lunak asli. Oleh sebab itu, apabila desa tidak bisa menjalin kerjasama untuk mendapatkan peranti lunak asli yang dibutuhkan, salah satu alternatif yang bisa dicoba adalah dengan menggunakan peranti lunak gratis dengan sistem *open-source*. Peranti lunak *open-source* pada umumnya dikembangkan oleh komunitas dengan tujuan untuk memberikan alternatif bagi masyarakat yang tidak dapat memiliki peranti lunak berlisensi komersil (Pratiwi et al., 2020).

Jawaban dari pertanyaan kedua merujuk kembali pada penggunaan peranti lunak anti virus. Saat ini sudah banyak dikembangkan peranti anti virus yang bisa digunakan oleh masyarakat sesuai dengan kebutuhannya. Tim pengabdi memberikan saran kepada penanya untuk mencoba melakukan pemindaian sistem terlebih dahulu dengan anti virus. Apabila virus dimaksud belum bisa disingkirkan, penanya dapat mengirimkan tangkapan layar perangkatnya yang terjangkit agar solusinya dapat ditemukan bersama.

### 3.4. Pembahasan

Berdasarkan rangkaian kegiatan abdimas yang telah dilakukan, terlihat bahwa pemahaman peserta pada dasarnya masih cukup rendah dalam hal keamanan siber. Peserta belum memahami konsep-konsep dasar yang tidak rumit dalam kajian keamanan siber. Walaupun begitu, ketika mencoba mempraktikkan, terlihat bahwa para peserta sudah cukup memahami bagaimana satu aplikasi bekerja untuk meningkatkan keamanan yang dimiliki dalam ruang siber. Hal ini menunjukkan bahwa peserta pengabdian belum memiliki pemahaman dasar tentang keamanan siber, namun telah memahami perangkat atau alat yang dapat digunakan untuk meningkatkan keamanan sibernya masing-masing.

Sistem keamanan siber yang digunakan oleh perangkat Desa Baros untuk mengamankan perangkat komputer dan akun yang dimiliki oleh Desa Baros cenderung masih minim. Komputer yang menjadi inventaris desa telah dilindungi oleh kata sandi, namun pengelola belum memasang aplikasi tambahan yang dapat memperkuat sistem keamanan siber di tingkat desa.

Kendala utama dari penguatan sistem keamanan siber yang ada di desa adalah kendala biaya dan prioritas. Selama ini belum pernah dilakukan penganggaran terkait peranti lunak. Permasalahan penganggaran merupakan permasalahan yang lazim ditemui dalam hal pengembangan sistem teknologi informasi dan komunikasi di institusi, termasuk dalam pengembangan kemampuan kemanan siber (Oktaviani & Silvia, 2021). Hal ini juga diperburuk dengan pola pikir bahwa warga bisa mendapatkan peranti lunak dengan gratis dengan mengunduh dari situs-situs yang tidak kredibel. Untuk mengatasi hal tersebut, tim pengabdi mengusulkan untuk menggunakan aplikasi sumber terbuka atau open source. Aplikasi sumber terbuka pada umumnya merupakan aplikasi yang dikembangkan oleh komunitas dan disebarkan secara cuma-cuma. Dengan menggunakan aplikasi sumber terbuka, maka pengguna dapat menghemat biaya namun tetap mendapatkan aplikasi dengan sistem keamanan yang mumpuni. Namun, perlu digarisbawahi bahwa banyak aplikasi sumber terbuka yang memiliki kurva belajar yang cenderung curam, sehingga pengguna perlu belajar ekstra keras dalam menggunakan aplikasi tersebut.

Secara umum dapat disampaikan bahwa kegiatan pengabdian kepada masyarakat yang dilakukan oleh tim pengabdi telah berhasil dalam membangun pola pikir digital secara umum bagi para pengelola situs desa dan media sosial Desa Baros. Secara khusus, tim pengabdi juga telah berhasil memberikan pemahaman kepada para pengelola situs desa dan media sosial Desa Baros tentang pentingnya peningkatan keamanan siber bagi aset digital yang dimiliki oleh institusi. Lebih lanjut, pengabdian ini juga berhasil memberikan rangkaian langkah-langkah peningkatan kemanan digital yang dapat dilakukan oleh pengelola situs desa dan media sosial Desa Baros.

## 4. KESIMPULAN

Pelatihan peningkatan keterampilan keamanan siber bagi pengelola situs desa dan media sosial Desa Baros berjalan dengan lancar tanpa kendala berarti. Setelah pelatihan peserta dapat memahami dengan baik konsep-konsep dasar dan juga praktek dasar terbaik dalam membangun sistem keamanan siber bagi situs desa dan media sosial Desa Baros. Ada pun ke depannya permasalahan keamanan siber perlu menjadi perhatian bagi pemerintah hingga ke level terkecil mengingat saat ini proses pemerintahan didorong untuk dilakukan secara digital. Tim pengabdi pun tidak serta merta melepas peserta setelah pelatihan, namun tim pengabdi terus melakukan pemantauan secara jarak jauh terkait pengelolaan situs desa dan media sosial yang dimiliki Desa Baros melalui kelompok WhatsApp. Kolaborasi lebih intens dapat terjadi ke depan dalam membangun sistem keamanan siber yang dimiliki oleh Desa Baros seperti melakukan pengecekan secara langsung ke lapangan dan mengukur pertahanan siber yang dimiliki oleh Desa Baros.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Pembangunan Nasional Veteran Jakarta yang telah memberi dukungan **finansial** terhadap pengabdian ini.

## DAFTAR PUSTAKA

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Nurchim, N., & Nofikasari, I. (2018). Analisis Model Pengembangan Telecenter Guna Mewujudkan Desa Pintar di Indonesia. *Fountain of Informatics Journal*, *3*(2), 36. https://doi.org/10.21111/fij.v3i2.2466

Oktaviani, P. B., & Silvia, A. (2021). Strategi Keamanan Siber Malaysia. *Jurnal Kajian Ilmiah*, *21*(1), 69–84. https://doi.org/10.31599/jki.v21i1.447

Pratiwi, D., Santoso, G. B., Mardianto, I., Sediyono, A., & Rochman, A. (2020). Pengelolaan Pengelolaan Konten Web Menggunakan Wordpress, Canva dan Photoshop untuk Guru-Guru Wilayah Jakarta. *Abdihaz: Jurnal Ilmiah Pengabdian Pada Masyarakat*, *2*(1), 11. https://doi.org/10.32663/abdihaz.v2i1.1093

Revilia, D., & Irwansyah, N. (2020). Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness. *JURNAL PENELITIAN KOMUNIKASI DAN OPINI PUBLIK*, *24*(1). https://doi.org/10.33299/jpkop.24.1.2375

Rohith, C., & Kaur, G. (2021). A Comprehensive Study on Malware Detection and Prevention Techniques used by Anti-Virus. *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, 429–434. https://doi.org/10.1109/ICIEM51511.2021.9445322

Saefudin. (2022). Tiga Hal Penting dalam Transformasi Digital Desa, Apa Saja? *Ditjen Aptika*. https://aptika.kominfo.go.id/2022/10/tiga-hal-penting-dalam-transformasi-digital-desa-apa-saja/

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759. https://doi.org/10.1007/s10207-019-00429-y