BADAN SIBER DAN SANDI NEGARA

PUSAT PENGEMBANGAN SUMBER DAYA MANUSIA

Jalan Raya Muchtar No.70, Kel. Duren Mekar, Kec. Bojong Sari, Depok 16518

Telepon (0251) 8618976, Faksimile (0251) 8617580

***Website*: https://pusbangsdm.bssn.go.id , *E-mail*: pusbang.sdm@bssn.go.id**

Depok, 14 Juli 2022

Nomor : 2688/BSSN/P3/DL.07.01/07/2022
Klasifikasi : Biasa
Lampiran : Satu berkas
Hal : Revisi Rencana Penyelenggaraan Pelatihan Peningkatan Kompetensi SDM Pengelola Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) Pada K/L/D T.A. 2022

Yth. Pejabat sesuai Daftar Alamat (Lampiran I)

di -

Tempat

1. Dasar :
   a. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
   b. Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
   c. Undang-Undang Republik Indonesia Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara;
   d. Undang-Undang Republik Indonesia Nomor 23 Tahun 2014 Tentang Pemerintahan Daerah;
   e. Peraturan Pemerintah Republik Indonesia Nomor 61 Tahun 2010 tentang Pelaksanaan UU Nomor 14 Tahun 2008 tentang KIP (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
   f. Peraturan Pemerintah Republik Indonesia Nomor 17 Tahun 2020 tentang Perubahan atas Peraturan Pemerintah Nomor 11 Tahun 2017 tentang Manajemen Pegawai Negeri Sipil;
   g. Peraturan Presiden Republik Indonesia Nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
   h. Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara;
   i. Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital;
   j. Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2021 tentang Pelatihan Keamanan Siber dan Persandian;

k. DIPA Badan Siber dan Sandi Negara T.A. 2022;
l. Program Kerja Pusbang SDM Badan Siber dan Sandi Negara T.A. 2022;
m. Surat Kepala Badan Siber dan Sandi Negara Nomor 1630/BSSN/P3/DL.07.01/04/2022 Tanggal 18 April 2022 Tentang Rencana Penyelenggaraan Pelatihan Peningkatan Kompetensi SDM Pengelola Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) T.A. 2022.
n. Surat Kepala Badan Siber dan Sandi Negara Nomor 1631/BSSN/P3/DL.07.01/04/2022 Tanggal 18 April 2022 Tentang Rencana Penyelenggaraan Pelatihan Peningkatan Kompetensi SDM Pengelola Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) T.A. 2022.

2. Sehubungan dengan dasar tersebut, disampaikan hal-hal sebagai berikut :
   a. Badan Siber dan Sandi Negara pada T.A. 2022 akan menyelenggarakan Pelatihan Peningkatan Kompetensi SDM Pengelola Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) melalui pelatihan ***Certified Secure Computer User*** (**CSCU**) secara **daring** sesuai dengan surat Surat Kepala Badan Siber dan Sandi Negara Nomor 1630/BSSN/P3/DL.07.01/04/2022 dan Nomor 1631/BSSN/P3/DL.07.01/04/2022 Tanggal 18 April 2022 Tentang Rencana Penyelenggaraan Pelatihan Peningkatan Kompetensi SDM Pengelola Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) T.A. 2022.

   b. Terdapat **perubahan** kegiatan pelatihan tersebut menjadi pelatihan *Certified Secure Computer User* (CSCU) secara daring **ditambah** pelatihan *Vulnerability Assessment Analyst* (VAA), pelatihan *Web Application Penetration test* (WAPT) dan pelatihan penanganan insiden siber secara **luring** di Pusat Pengembangan Sumber Daya Manusia (SDM) Badan Siber dan Sandi Negara di Jl. Raya Muchtar No.70, Bojongsari Lama, Kecamatan Bojongsari, Kota Depok, Jawa Barat 16516.

   c. Pelaksanaan pelatihan dibagi menjadi dua gelombang dengan rincian sebagai berikut:
      1) Pelatihan gelombang I untuk 88 orang pada tanggal 22 - 31 Agustus 2022;
      2) Pelatihan gelombang II untuk 87 orang pada tanggal 19 – 28 September 2022;

   Berikut tabel penjelasan perubahan rencana pelatihan SPBE:

SEMULA	MENJADI
MATERI PELATIHAN	
Certified Secure Computer User (CSCU)	• Materi *Certified Secure Computer User* (CSCU) • Materi *Vulnerability Assessment Analyst* (VAA) • Materi *Web Application Penetration test* (WAPT)

SEMULA	MENJADI
	• Materi Penanganan Insiden Siber

WAKTU PELAKSANAAN		
Gelombang I	Prioritas Peserta dari Wilayah Indonesia Timur) : tanggal 28 – 30 Juni 2022; Metode : **daring**	Target peserta 88 orang dari seluruh K/L/D pada tanggal 22 - 31 Agustus 2022; • Materi VAA dilaksanakan pada 22-23 Agustus 2022 secara **luring** • Materi WAPT dilaksanakan pada 24-25 Agustus 2022 secara **luring** • Materi Penanganan Insiden Siber dilaksanakan pada 25-26 Agustus 2022 secara **luring**. • Materi CSCU dilaksanakan pada 29-31 Agustus 2022 secara **daring**
Gelombang II	Prioritas Peserta dari Wilayah Indonesia Tengah) : tanggal 05 - 07 Juli 2022; Metode : **daring**	Target peserta 87 orang dari seluruh K/L/D pada tanggal 19 – 28 September 2022; • Materi VAA dilaksanakan pada 19-20 September 2022 secara **luring** • Materi WAPT dilaksanakan pada 21-22 September 2022 secara **luring** • Materi Penanganan Insiden Siber dilaksanakan pada 22-23 September 2022 secara **luring**. • Materi CSCU dilaksanakan pada 26-28 September 2022 secara **daring**
Gelombang III	Prioritas Peserta dari Wilayah Indonesia Barat, Kementerian, dan Lembaga: tanggal 12 - 14 Juli 2022; Metode : **daring**	tidak ada

d. Kegiatan ini bertujuan untuk meningkatkan kompetensi SDM KSS pengelola Keamanan SPBE yang mahir dalam perlindungan data pribadi dan mampu dalam mendeteksi kerentanan serta mampu dalam menangani insiden siber.

e. Persyaratan peserta yaitu:
   1) ASN;
   2) Sudah bekerja atau sanggup bekerja pada lingkup keamanan informasi dan atau persandian;
   3) Mampu dan terbiasa menggunakan perangkat komputer dan atau *smartphone;*
   4) Membawa laptop dengan spesifikasi minimal prosesor Intel Core i5 dan ram 4 GB atau setara;
   5) **Bersedia** dan **wajib** mengikuti seluruh rangkaian pelatihan.

f. Calon peserta pelatihan **wajib** mengisi biodata pada link pendaftaran pelatihan Gelombang ke I pada tautan berikut: **https://survey.bssn.go.id/619372?newtest=Y&lang=id** atau **https://s.id/spbesatu**

g. Calon peserta pelatihan **wajib** mengisi biodata pada link pendaftaran pelatihan Gelombang ke II pada tautan berikut: **https://survey.bssn.go.id/884333?newtest=Y&lang=id** atau **https://s.id/spbedua**

h. Selanjutnya Pusbang SDM BSSN akan menyampaikan **pemberitahuan** melalui media komunikasi kepada calon peserta yang telah memenuhi persyaratan dan alokasi jumlah peserta, berdasarkan daftar peserta yang diusulkan dari masing-masing alamat.

i. Peserta **tidak** dipungut biaya pelatihan. **Biaya transportasi peserta ditanggung oleh Instansi masing-masing peserta pelatihan**. Selama kegiatan pelatihan **luring**, peserta diasramakan di Pusat Pengembangan SDM BSSN, Bojongsari Depok.

3. Informasi tentang pelaksanaan pelatihan BSSN T.A. 2022 tersebut dapat menghubungi:
   Email : pusbang.sdm@bssn.go.id
   No. WhatsApp : 0813-1688-9983 (Diklat Tekfung, Pusbang SDM BSSN)
4. Demikian disampaikan, atas perhatian dan kerjasamanya diucapkan terima kasih.

a.n. Kepala Badan Siber dan Sandi Negara

Ditandatangani secara elektronik oleh:
KEPALA PUSAT PENGEMBANGAN SUMBER DAYA MANUSIA

DAME RIA MUNTHE, S.E.
Pembina Utama Madya (IV/d)

Tembusan :

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi se-Indonesia;
3. Wakil Kepala BSSN;
4. Sekretaris Jenderal Kemendagri;
5. Sekretaris Utama BSSN;
6. Bupati/Walikota Kabupaten/Kota se-Indonesia;
7. Sekretaris Daerah Provinsi se-Indonesia;
8. Sekretaris Daerah Kabupaten/Kota se-Indonesia;
9. Inspektur BSSN.

Lampiran I Surat Kepala BSSN
Nomor : 2688/BSSN/P3/DL.07.01/07/2022
Tanggal : 14 Juli 2022

DAFTAR ALAMAT SURAT

1. Sekretaris Jenderal/Sekretaris Utama/Sekretaris Kementerian/Lembaga;
2. Kepala Dinas Komunikasi dan Informatika Provinsi se-Indonesia;
3. Kepala Dinas Komunikasi dan Informatika Kabupaten/Kota se-Indonesia.

Lampiran II Surat Kepala BSSN
Nomor : 2688/BSSN/P3/DL.07.01/07/2022.
Tanggal : 14 Juli 2022

BIODATA CALON PESERTA PELATIHAN SPBE
GELOMBANG KE-.....

1. NAMA : .....
2. N I P : .....
3. TEMPAT/TANGGAL LAHIR : .....
4. PANGKAT/GOLONGAN : .....
5. PENDIDIKAN TERAKHIR : .....
6. JABATAN : .....
7. ASAL INSTANSI : .....
8. NOMOR TELEPON
   - HP : .....
   - KANTOR : .....
   - FAX : .....
9. ALAMAT EMAIL :
   - PRIBADI : .....
   - KANTOR : .....

.....,.....,.....

MENGETAHUI ATASAN CALON PESERTA PELATIHAN

(.....) (.....)

Catatan:

- Mohon formulir ini dilengkapi oleh peserta dan diunggah ke dalam tautan pendaftaran yang tersedia di dalam surat ini

Lampiran III Surat Kepala BSSN
Nomor : 2688/BSSN/P3/DL.07.01/07/2022.
Tanggal : 14 Juli 2022

REKOMENDASI PIMPINAN

1. NAMA : .....
2. N I P : .....
4. PANGKAT/GOLONGAN : .....
5. JABATAN : .....
6. ASAL INSTANSI : .....

Memberikan rekomendasi kepada:

1. NAMA : .....
2. N I P : .....
4. PANGKAT/GOLONGAN : .....
5. JABATAN : .....
6. ASAL INSTANSI : .....

untuk mengikuti pelatihan **SPBE GELOMBANG KE-.....** yang diselenggarakan oleh Pusat Pengembangan Sumber Daya Manusia Badan Siber dan Sandi Negara.

Demikian surat rekomendasi ini saya buat, agar dapat digunakan sebagaimana mestinya.

.....,.....,.....

ATASAN

(.....)

Catatan:

- Mohon formulir ini dilengkapi oleh peserta dan diunggah ke dalam link pendaftaran yang tersedia di dalam surat ini.

Lampiran IV Surat Kepala BSSN
Nomor : 2688/BSSN/P3/DL.07.01/07/2022.
Tanggal : 14 Juli 2022

FORM KOMITMEN PARTISIPASI
KEGIATAN PELATIHAN PUSBANG SDM BSSN TAHUN 2022

Formulir ini untuk diisi (diketik atau tulis tangan dengan jelas) kemudian dikirim ke penyelengara pelatihan melalui email pelatihan.tekfung@bssn.go.id

Saya yang bertandatangan di bawah ini:

Nama Lengkap (Sesuai KTP) :

Tempat/Tanggal Lahir :

N I K :

N I P :

Pangkat / Golongan :

Jabatan :

No HP Aktif :

Email Aktif :

Alamat Domisili :

Pelatihan yang akan diikuti : Pelatihan **SPBE GELOMBANG KE- .....**

Menyatakan:

1. Bersedia mengikuti seluruh tahapan pelatihan sejak awal hingga selesai;
2. Bersedia menjadi peserta pelatihan yang pembiayaannya bersumber dari anggaran pemerintah;
3. Bersedia memenuhi persyaratan administratif serta Syarat dan Ketentuan yang berlaku;
4. Bersedia memenuhi Kewajiban dan Tata Tertib sebagai peserta pelatihan;
5. Bersedia menerima dan tidak akan mengganggu-gugat segala keputusan final penyelenggara pelatihan;
6. Mengerti dan setuju bahwa konten pelatihan digunakan *hanya* untuk kebutuhan pelatihan di BSSN.
7. Segala konten pelatihan termasuk tidak terbatas pada soal tes substansi, soal kuis, soal *mid exam*, soal *final exam*, materi pelatihan, video, gambar dan kode ini mengandung Kekayaan Intelektual, peserta tunduk kepada undang-undang hak cipta, merek dagang atau hak kekayaan intelektual lainnya. Tidak mereproduksi, memodifikasi, menyebarluaskan, atau mengeksploitasi konten ini dengan cara atau bentuk apapun tanpa persetujuan tertulis dari penyelenggara pelatihan.
8. Peserta yang terbukti melakukan pelanggaran ini akan dicabut hak sebagai peserta pelatihan dan akan menerima konsekuensi sesuai aturan yang berlaku.
9. Bersedia memberikan informasi pribadi yang tercantum dalam form pendaftaran kepada penyelenggara pelatihan untuk kepentingan pelaksanaan pelatihan dan pasca pelatihan.
10. Tidak terlibat dalam paham radikal dan terorisme.

11. Tidak terlibat penyalahgunaan narkotika, obat-obatan terlarang dan kriminal.

Demikian Surat Pernyataan ini dibuat dengan sebenarnya secara sadar dan tanpa paksaan. Apabila dikemudian hari pernyataan ini terbukti tidak benar, maka saya bersedia untuk dicabut haknya sebagai peserta pelatihan dan menerima sanksi sesuai ketentuan Pusbang SDM Badan Siber dan Sandi Negara.

……., ….. 2022

Atasan Langsung,	Peserta Pelatihan,
……..……	……..……

Lampiran V Surat Kepala BSSN
Nomor : 2688/BSSN/P3/DL.07.01/07/2022
Tanggal : 14 Juli 2022

RUNDOWN KEGIATAN PELATIHAN PENINGKATAN KOMPETENSI SDM PENGELOLA KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) PADA K/L/D GELOMBANG KE 1

HARI/TGL	WAKTU	MATERI PEMBELAJARAN	METODE
SENIN	08.00 – 08.45	Upacara Pembukaan	Luring di Pusbang SDM BSSN, Bojongsari Depok
22 Agustus 2022	08.45 – 09.30	Pengarahan program	
	09.30 – 09.45	*Coffee Break*	
	09.45 – 11.15	Pre-Test	
	11.15 – 12.00	*Vulnerability Assessment Fundamental*	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 13.45	*Vulnerability Assessment Fundamental*	
	13.45 – 15.15	*Vulnerability Assessment* pada Aplikasi Web	
	15.15 – 15.30	*Coffee Break*	
	15.30 – 17.00	*Vulnerability Assessment* pada Sistem Operasi Windows	
SELASA	08.00 – 09.30	*Vulnerability Assessment* pada Sistem Operasi Linux	Luring di Pusbang SDM BSSN, Bojongsari Depok
23 Agustus 2022	09.30 – 10.15	*Vulnerability Assessment* pada Jaringan	
	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	*Vulnerability Assessment* pada Jaringan	
	11.45 – 12.00	*Vulnerability Assessment* pada Aplikasi Mobile	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 13.45	*Vulnerability Assessment* pada Aplikasi Mobile	
	13.45 – 15.15	Perhitungan Nilai Risiko	
	15.15 – 15.30	*Coffee Break*	
	15.30 – 17.00	Penyusunan Laporan *Vulnerability Assessment*	
RABU	08.00 – 09.30	*Web Application Penetration test Fundamental*	Luring di Pusbang SDM BSSN, Bojongsari Depok
24 Agustus 2022	09.30 – 10.15	*Basic Linux and Web Application*	
	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	*Basic Linux and Web Application*	
	11.45 – 12.00	*Vulnerability Assessment* pada *Web Application*	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 15.15	*Web Application Exploitation*	
	15.15 – 15.30	*Coffee Break*	
	15.30 – 17.00	*Web Application Exploitation*	
KAMIS	08.00 – 10.15	*Web Application Exploitation*	Luring di Pusbang SDM BSSN, Bojongsari Depok
25 Agustus 2022	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	*Web Application Exploitation*	
	11.15 – 12.00	*Post Exploitation and Report*	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 13.45	*Post Exploitation and Report*	
	13.45 – 14.30	Pengenalan Penanganan Insiden Siber	
	14.30 – 15.15	Persiapan Tanggap Insiden	

HARI/TGL	WAKTU	MATERI PEMBELAJARAN	METODE
	15.15 – 15.30	*Coffee Break*	
	15.30 – 16.15	*Fundamental* Identifikasi dan Analisis, *Containment, Eradication*, Pemulihan Insiden	
Jumat	08.00 – 08.45	Pemulihan Insiden	Luring di Pusbang SDM BSSN, Bojongsari Depok
26 Agustus 2022	08.45 – 09.30	Aktifitas Pasca Insiden dan Pelaporan	
	09.30 – 10.15	Studi Kasus *Email Phising*: Identifikasi dan Analisis, *Containment, Eradication*	
	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	Studi Kasus *Data Breach*: Identifikasi dan Analisis, *Containment, Eradication*	
	11.15 – 13.15	*Lunch Break*	
	13.15 – 14.00	Ceramah Substantif	
	14.00 – 15.30	Evaluasi (Post-Test)	
Senin	08.00 – 12.00	Materi *Secure Computer User*	Daring
29 Agustus 2022	12.00 – 13.00	*Lunch Break*	
	13.00 – 16.00	Materi *Secure Computer User*	
Selasa	08.00 – 12.00	Materi *Secure Computer User*	Daring
30 Agustus 2022	12.00 – 13.00	*Lunch Break*	
	13.00 – 16.00	Materi *Secure Computer User*	
Rabu	08.00 – 11.00	Evaluasi SCU	Daring
31 Agustus 2022	11.00 – 11.45	Rapat Kelulusan	
	11.45 – 13.00	*Lunch Break*	
	13.00 – 14.00	Upacara Penutupan	

RUNDOWN KEGIATAN PELATIHAN PENINGKATAN KOMPETENSI SDM PENGELOLA KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) PADA K/L/D GELOMBANG KE-2

HARI/TGL	WAKTU	MATERI PEMBELAJARAN	METODE
SENIN	08.00 – 08.45	Upacara Pembukaan	Luring di Pusbang SDM BSSN, Bojongsari Depok
19 September 2022	08.45 – 09.30	Pengarahan program	
	09.30 – 09.45	*Coffee Break*	
	09.45 – 11.15	Pre-Test	
	11.15 – 12.00	*Vulnerability Assessment Fundamental*	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 13.45	*Vulnerability Assessment Fundamental*	
	13.45 – 15.15	*Vulnerability Assessment* pada Aplikasi Web	
	15.15 – 15.30	*Coffee Break*	
	15.30 – 17.00	*Vulnerability Assessment* pada Sistem Operasi Windows	
SELASA	08.00 – 09.30	*Vulnerability Assessment* pada Sistem Operasi Linux	Luring di Pusbang SDM BSSN, Bojongsari Depok
20 September 2022	09.30 – 10.15	*Vulnerability Assessment* pada Jaringan	
	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	*Vulnerability Assessment* pada Jaringan	
	11.45 – 12.00	*Vulnerability Assessment* pada Aplikasi Mobile	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 13.45	*Vulnerability Assessment* pada Aplikasi Mobile	
	13.45 – 15.15	Perhitungan Nilai Risiko	
	15.15 – 15.30	*Coffee Break*	
	15.30 – 17.00	Penyusunan Laporan *Vulnerability Assessment*	
RABU	08.00 – 09.30	*Web Application Penetration test Fundamental*	Luring di Pusbang SDM BSSN, Bojongsari Depok
21 September 2022	09.30 – 10.15	*Basic Linux and Web Application*	
	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	*Basic Linux and Web Application*	
	11.45 – 12.00	*Vulnerability Assessment* pada *Web Application*	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 15.15	*Web Application Exploitation*	
	15.15 – 15.30	*Coffee Break*	
	15.30 – 17.00	*Web Application Exploitation*	
KAMIS	08.00 – 10.15	*Web Application Exploitation*	Luring di Pusbang SDM BSSN, Bojongsari Depok
22 September 2022	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	*Web Application Exploitation*	
	11.15 – 12.00	*Post Exploitation and Report*	
	12.00 – 13.00	*Lunch Break*	
	13.00 – 13.45	*Post Exploitation and Report*	
	13.45 – 14.30	Pengenalan Penanganan Insiden Siber	
	14.30 – 15.15	Persiapan Tanggap Insiden	
	15.15 – 15.30	*Coffee Break*	
	15.30 – 16.15	*Fundamental* Identifikasi dan Analisis, *Containment, Eradication*, Pemulihan Insiden	
Jumat	08.00 – 08.45	Pemulihan Insiden	

HARI/TGL	WAKTU	MATERI PEMBELAJARAN	METODE
23 September 2022	08.45 – 09.30	Aktifitas Pasca Insiden dan Pelaporan	Luring di Pusbang SDM BSSN, Bojongsari Depok
	09.30 – 10.15	Studi Kasus *Email Phising*: Identifikasi dan Analisis, *Containment, Eradication*	
	10.15 – 10.30	*Coffee Break*	
	10.30 – 11.15	Studi Kasus *Data Breach*: Identifikasi dan Analisis, *Containment, Eradication*	
	11.15 – 13.15	*Lunch Break*	
	13.15 – 14.00	Ceramah Substantif	
	14.00 – 15.30	Evaluasi (Post-Test)	
Senin	08.00 – 12.00	Materi *Secure Computer User*	Daring
26 September 2022	12.00 – 13.00	*Lunch Break*	
	13.00 – 16.00	Materi *Secure Computer User*	
Selasa	08.00 – 12.00	Materi *Secure Computer User*	Daring
27 September 2022	12.00 – 13.00	*Lunch Break*	
	13.00 – 16.00	Materi *Secure Computer User*	
Rabu	08.00 – 11.00	Evaluasi SCU	Daring
28 September 2022	11.00 – 11.45	Rapat Kelulusan	
	11.45 – 13.00	*Lunch Break*	
	13.00 – 14.00	Upacara Penutupan	

Lampiran VI Surat Kepala BSSN
Nomor : 2688/BSSN/P3/DL.07.01/07/2022
Tanggal : 14 Juli 2022

PENJABARAN KURIKULUM PELATIHAN PENINGKATAN KOMPETENSI SDM PENGELOLA KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) PADA K/L/D

A. MATERI *CERTIFIED SECURE COMPUTER USER*

No.	Materi Pokok	Sub Materi Pokok		JP	Deskripsi
1.	*Introduction To Data Security*	a.	*Data–Digital Building Blocks*	2	Mata pelatihan ini membahas tentang blok data digital, pentingnya data di zaman informasi, ancaman terhadap data, keamanan data, kerugian terhadap serangan serta implementasi keamanan komputer
		b.	*Importance of Data in the Information Age*		
		c.	*Threats to Data*		
		d.	*Data Security*		
		e.	*Potential Losses Due to Security Attacks*		
		f.	*Implementing Security*		
2.	*Securing Operating Systems*	a.	*Guidelines To Secure Windows*	2	Mata pelatihan ini membahas tentang keamanan sistem operasi windows dan macOS X
		b.	*Guidelines To Secure macOS X*		
3.	*Malware and Antiviruses*	a.	*What is Malware*	3	Mata pelatihan ini membahas tentang definisi malware, tipe malware, infeksi malware, antivirus serta cara kerja antivirus
		b.	*Types Of Malware*		
		c.	*Symptoms Of Malware Infection*		
		d.	*Antivirus*		
		e.	*Configuring and Using Antivirus Software*		
		f.	*How To Test If an Antivirus is Working*		
4.	*Internet Security*	a.	*Understanding Web Browser Concepts*	1	Mata pelatihan ini membahas tentang konsep internet, keamanan pengiriman pesan di internet serta keselamatan anak saat online di dunia maya
		b.	*Understanding IM Security*		
		c.	*Understanding Child Online Safety*		
5.	*Security On Social Networking Sites*	a.	*Understanding Social Networking Concepts*	2	Mata pelatihan ini membahas tentang konsep jejaring sosial online, ancaman di media sosial, pengaturan keamanan facebook, pengaturan keamanan twitter
		b.	*Understanding Various Social Networking Security Threats*		
		c.	*Understanding Facebook Security Settings*		
		d.	*Understanding Twitter Security Settings*		
6.	*Securing Email Communications*	a.	*Understanding Email Security Concepts*	2	

No.	Materi Pokok	Sub Materi Pokok		JP	Deskripsi
		b.	*Understanding Various Email Security Threats*		Mata pelatihan ini membahas tentang konsep keamanan email, jenis ancaman email, serta prosedur pengamanan email
		c.	*Understanding Various Email Security Procedures*		
7.	*Securing Mobile Devices*	a.	*Understanding Mobile Device Security Concepts*	2	Mata pelatihan ini membahas tentang konsep keamanan perangkat mobile, ancaman terhadap perangkat mobile, prosedur keamanan perangkat mobile, metode pengamanan iphone dan ipad, pengamanan perangkat android, pengamanan perangkat windows serta utilitas keamanan mobile
		b.	*Understanding Threats To a Mobile Device*		
		c.	*Understanding Various Mobile Security Procedures*		
		d.	*Understanding How to Secure iPhone and iPad Devices*		
		e.	*Understanding How to Secure Android Devices*		
		f.	*Understanding How to Secure Windows Device*		
		g.	*Mobile Security Tools*		
8.	*Securing The Cloud*	a.	*The Concept of Cloud*	2	Mata pelatihan ini membahas tentang konsep *cloud*, cara kerja *cloud*, ancaman keamanan *cloud*, pengamanan terhadap ancaman keamanan *cloud*, privasi *cloud*, serta pemilihan penyedia layanan *cloud*
		b.	*How Cloud Works*		
		c.	*Threats To Cloud Security*		
		d.	*Safeguarding Against Cloud Security Threats*		
		e.	*Cloud Privacy Issues*		
		f.	*Addressing Cloud Privacy Issues*		
		g.	*Choosing a Cloud Service Provider*		
9.	*Securing Network Connections*	a.	*Understanding Various Networking Concepts*	2	Mata pelatihan ini membahas tentang konsep pengamanan jaringan, menerapkan jaringan nirkabel di sistem operasi windows, menerapakan jaringan nirkabel di sistem operasi mac, pengamanan jaringan nirkabel serta pengukuran keamanan koneksi jaringan
		b.	*Understanding Setting Up a Wireless Network in Windows*		
		c.	*Understanding Setting Up a Wireless Network in Mac*		
		d.	*Understanding Threats to Wireless Network Security and Countermeasures*		
		e.	*Measures to Secure Network Connections*		
10.	*Data Backup and Disaster Recovery*	a.	*Data Backup Concepts*	3	Mata pelatihan ini membahas tentang konsep *backup* data, tipe *backup* data, prosedur *backup* dan pemulihan data di sistem operasi windows, prosedur *backup* dan pemulihan data di sistem operasi macOS X, serta pengamanan penghapusan data
		b.	*Types of Data Backups*		
		c.	*Windows Backup and Restore Procedures*		
		d.	*macOS X Backup and Restore Procedures*		
		e.	*Understanding Secure Data Destruction*		
TOTAL JAM PELAJARAN (JP)				**21**	

B. MATERI *VULNERABILITY ASSESSMENT ANALYST*

No.	Materi Pokok		Sub Materi Pokok	JP	Deskripsi
1	*Vulnerability Assessment Fundamental*		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang konsep vulnerability assessment, perangkat *Vulnerability Assessment* dan tinjauan efektifitas kontrol
		2.1	Konsep vulnerability assessment;		
		2.2	Pengenalan perangkat vulnerability assessment;		
		2.3	Manajemen konfigurasi dan tinjauan efektifitas kontrol		
2	*Vulnerability Assessment* pada Aplikasi Web		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang *framework* aplikasi web, *information gathering* pada aplikasi web, *Vulnerability Assessment* pada aplikasi web dan analisis hasil *Vulnerability Assessment* pada aplikasi web
		3.1	*Framework* aplikasi web;		
		3.2	*Information gathering* pada aplikasi web;		
		3.3	*Vulnerability Assessment* pada aplikasi web;		
		3.4	Analisis hasil *Vulnerability Assessment* pada aplikasi web		
3	*Vulnerability Assessment* pada Sistem Operasi Windows		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang pengenalan karateristik sistem operasi windows, *information gathering* pada sistem operasi windows, perangkat *Vulnerability Assessment* pada sistem operasi windows dan analisis hasil *Vulnerability Assessment* pada sistem operasi windows
		4.1	Pengenalan karateristik sistem operasi windows;		
		4.2	*Information gathering* pada sistem operasi windows;		
		4.3	*Vulnerability Assessment* pada sistem operasi windows;		
		4.4	Analisis hasil *Vulnerability Assessment* pada sistem operasi windows.		
4	*Vulnerability Assessment* pada Sistem Operasi Linux		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang dasar-dasar sistem operasi linux, *information gathering* pada sistem operasi linux, perangkat *Vulnerability Assessment* pada sistem operasi linux dan analisis hasil *Vulnerability Assessment* pada sistem operasi linux
		5.1	Dasar-dasar sistem operasi linux;		
		5.2	*Information gathering* pada sistem operasi linux;		
		5.3	*Vulnerability Assessment* pada sistem operasi linux;		
		5.4	Analisis hasil *Vulnerability Assessment* pada sistem operasi linux.		
5	*Vulnerability Assessment* pada Jaringan		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang dasar-dasar jaringan, *information gathering* pada jaringan, perangkat *Vulnerability Assessment* pada jaringan dan analisis hasil *Vulnerability Assessment* pada jaringan
		6.1	Dasar-dasar jaringan;		
		6.2	*Information gathering* pada jaringan;		
		6.3	*Vulnerability Assessment* pada jaringan;		
		6.4	Analisis tools *Vulnerability Assessment* pada jaringan.		

No.	Materi Pokok	Sub Materi Pokok		JP	Deskripsi
6	*Vulnerability Assessment* pada Aplikasi Mobile		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang dasar-dasar aplikasi mobile, proses *vulnerability analysis* pada aplikasi mobile, perangkat *Vulnerability Assessment* pada aplikasi mobile dan analisis hasil *Vulnerability Assessment* pada aplikasi mobile
		7.1	Dasar-dasar aplikasi mobile;		
		7.2	Proses *vulnerability analysis* pada aplikasi mobile;;		
		7.3	Perangkat *Vulnerability Assessment* pada aplikasi mobile;		
		7.4	Analisis hasil *Vulnerability Assessment* pada aplikasi mobile.		
7	Perhitungan Nilai Risiko		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang konsep proses verifikasi dan penilaian kerentanan, penilaian risiko serta penilaian kerentanan
		8.1	Konsep dasar proses verifiaksi dan penilaian risiko;		
		8.2	Penilaian risiko;		
		8.3	Verifikasi dan penilaian ancaman.		
8	Penyusunan Laporan Vulnerability Assessment		Sub Materi Pokok :	2	Mata Pelatihan ini membahas pentingnya pelaporan *Vulnerability Assessment* dan penyusunan laporan *vulnerability assessment*
		9.1	Pengantar penyusunan laporan vulnerability assessment;		
		9.2	Penyusunan laporan vulnerability assessment.		
TOTAL JAM PELAJARAN (JP)				**16**	

C. MATERI *WEB APPLICATION PENETRATION TEST*

No.	Materi Pokok	Sub Materi Pokok		JP	Deskripsi
1	*Web Application Penetration test Fundamental*		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang gambaran umum *penetration test*, termonologi dalam *penetration test*, tahapan *penetration test* dan konfigurasi laboratorium
		2.1	Gambaran umum *penetration test*		
		2.2	Terminology dalam *penetration test*		
		2.3	Tahapan *penetration test*		
		2.4	Konfigurasi laboratorium		
2	*Basic Linux and Web Application*		Sub Materi Pokok :	2	Mata pelatihan ini membahas tentang basic linux dan basic *Web Application*
		3.1	Basic linux;		
		3.2	Basic *Web Application*		
3	*Vulnerability Assessment* pada *Web Application*		Sub Materi Pokok :	1	Mata Pelatihan ini membahas *Fundamental vulnerability assesment* pada aplikasi web, perangkat *vulnerability assesment* pada aplikasi web, tinjauan efektivitas kontrol dan laporan *vulnerability assesment*
		4.1	*Fundamental Vulnerability Assessment* pada aplikasi web		
		4.2	Perangkat *Vulnerability Assessment* pada aplikasi web		
		4.3	Tinjauan efektifitas kontrol		

No.	Materi Pokok	Sub Materi Pokok		JP	Deskripsi
4	*Web Application Exploitation*		Sub Materi Pokok :	9	Mata pelatihan ini membahas tentang teknik eksploitasi pada aplikasi web, teknik eksploitasi dalam risiko Injection, teknik eksploitasi dalam risiko *Broken Authentication*, teknik eksploitasi dalam risiko *Sensitive Data Exposure*, teknik eksploitasi dalam risiko XML *External Entities* (XEE), teknik eksploitasi dalam risiko *Broken Access Control*, teknik eksploitasi dalam risiko *Security Misconfiguration*, teknik eksploitasi dalam risiko *Cross Site Scripting* (XSS), teknik eksploitasi dalam risiko *Insecure Deserialization*, teknik eksploitasi dalam risiko *Using Computers with Known Vulnerabilities*, teknik eksploitasi dalam risiko *Logging and Monitoring*
		5.1	Teknik eksploitasi pada aplikasi web		
		5.2	Teknik eksploitasi dalam risiko *injection*		
		5.3	Teknik eksploitasi dalam risiko *broken authentication*		
		5.4	Teknik eksploitasi dalam risiko *sensitive data exposure*		
		5.5	Teknik eksploitasi dalam risiko xml *external entities*		
		5.6	Teknik eksploitasi dalam risiko *broken access control*		
		5.7	Teknik eksploitasi dalam risiko *security misconfiguration*		
		5.8	Teknik eksploitasi dalam risiko *cross site scripting*		
		5.9	Teknik eksploitasi dalam risiko *insecure deserialization*		
		5.10	Teknik eksploitasi dalam risiko *using components with known vulnerabilities*		
		5.11	Teknik eksploitasi dalam risiko *insufficient logging and monitoring*		
5	*Post Exploitation and Report*		Sub Materi Pokok :	2	Mata pelatihan ini membahas post *Exploitation* dan penyusunan laporan *penetration test*
		6.1	Post *Exploitation*		
		6.2	Penyusunan laporan *penetration test*		
TOTAL JAM PELAJARAN (JP)				**16**	

D. MATERI PENANGANAN INSIDEN SIBER

No.	Materi Pokok	Sub Materi Pokok		JP	Deskripsi
1	Pengenalan Penanganan Insiden Siber	a.	konsep dasar tanggap insiden siber;	1	Mata pelatihan ini membahas konsep dasar tanggap insiden; kebijakan dan perencanaan tanggap insiden; dan struktur dan peran tim tanggap insiden
		b.	kebijakan dan perencanaan tanggap insiden siber;		
		c.	struktur dan peran tim tanggap insiden siber.		
2	Persiapan Tanggap Insiden	a.	konsep persiapan tanggap insiden siber: 3 aspek;	1	Mata pelatihan ini membahas tentang konsep persiapan tanggap insiden, pembuatan prosedur persiapan tanggap insiden dan penanganan insiden (studi kasus)
		b.	prosedur penyiapan 3 aspek persiapan; dan		
		c.	penanganan insiden siber (studi kasus)		
3	*Fundamental* Identifikasi dan Analisis, *Containment, Eradication*, Pemulihan Insiden	a.	teknik dan prosedur serangan;	1	Mata pelatihan ini membahas tentang *Fundamental* teknik dan prosedur serangan; tanda-tanda serangan; tujuan dan fungsi *containment*; *eradication*; perencanaan pemulihan
		b.	tanda-tanda serangan;		
		c.	tujuan dan fungsi *containment*;		
		d.	*Fundamental eradication*;		

No.	Materi Pokok	Sub Materi Pokok		JP	Deskripsi
		e.	perencanaan pemulihan insiden; dan		insiden; dan memahami peningkatan kemampuan pemulihan
		f.	peningkatan kemampuan pemulihan		
4	Pemulihan Insiden (2 Studi Kasus)	a.	pemulihan sistem;	1	Mata Pelatihan ini membahas tentang tahapan pemulihan insiden
		b.	validasi sistem;		
		c.	pemulihan taktis; dan		
		d.	pemulihan strategis		
5	Aktifitas Pasca Insiden dan Pelaporan (2 Studi Kasus)	a.	aktifitas pasca insiden;	1	Mata pelatihan ini membahas tentang lesson learned aktifitas pasca insiden, serta koordinasi pasca insiden, dan berbagi informasi
		b.	pelaporan dan ringkasan eksekutif insiden; dan		
		c.	koordinasi dan information sharing.		
6	Studi Kasus *Email Phising*: Identifikasi dan Analisis, *Containment, Eradication*	a.	*data collection*;	1	Mata pelatihan ini membahas tentang identifikasi dan analisis (*data collection*), *containment* (isolasi komputer *compromised, preserving operability*) dan *eradication* pada studi kasus *email phishing*
		b.	isolasi komputer *compromised*;		
		c.	proses *preserving operability*; dan		
		d.	*eradication*.		
7	Studi Kasus *Data Breach*: Identifikasi dan Analisis, *Containment, Eradication*	a.	*data collection*;	1	Mata pelatihan ini membahas tentang identifikasi dan analisis (*data collection*), *containment* (isolasi komputer *compromised, preserving operability*) dan *eradication* pada studi kasus *Data Breach*
		b.	isolasi komputer *compromised*;		
		c.	proses *preserving operability*; dan		
		d.	*eradication*.		
8	Ceramah Substantif	a.	ceramah kebijakan penanganan insiden siber nasional; dan	1	Mata diklat ini membekali peserta dengan kemampuan menjelaskan kebijakan dan isu strategis pengelolaan CSIRT dan keamanan siber
		b.	ceramah perkembangan isu strategis penanganan insiden siber Nasional.		
TOTAL JAM PELAJARAN (JP)				8	