	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI PEMBANGUNAN MAKLUMAT DAN MALAYSIA Kod Dokumen: UPM/	Halaman: 1/6
		No. Semakan: 09
		No. Isu: 01
	POLISI PENGURUSAN KOD SUMBER	Tarikh: 31/01/2023


1. SKOP

Polisi ini bertujuan untuk menetapkan prinsip, tanggungjawab, dan tatacara pelaksanaan semakan kod dan pengekodan selamat dalam semua aktiviti pembangunan sistem, aplikasi dan perisian di PTPKM. Ia dirangka bagi menjamin keselamatan, kebolehpercayaan dan pematuhan terhadap keperluan kawal selia serta piawaian antarabangsa berkaitan keselamatan aplikasi. Skop polisi ini merangkumi:

- Semua sistem dan aplikasi yang dibangunkan secara dalaman oleh PTPKM atau pihak ketiga.
- Semua fasa dalam Kitaran Hayat Pembangunan Perisian (SDLC) termasuk reka bentuk, pembangunan, ujian, pengeluaran, dan penyelenggaraan.
- **Semakan kod manual (*peer review*) dan automatik (menggunakan alat SAST, DAST, dan IAST).**
- Pelaksanaan pengekodan selamat berdasarkan piawaian lain yang diluluskan oleh PTPKM.
- Semua kakitangan pembangunan, jurutera keselamatan, pengurus projek dan pembekal perisian.


2. TANGGUNGJAWAB

PERANAN	TANGGUNGJAWAB
Pasukan Pembangunan	Menulis kod yang selamat dan mematuhi keperluan PQC serta menjalankan semakan rakan setugas.
Ketua Pembangunan Sistem	Memastikan semua kod disemak sebelum pengeluaran dan memantau pematuhan.
Pegawai Keselamatan	Mengendalikan analisis keselamatan kod dan memberikan nasihat teknikal berkaitan risiko keselamatan.
Pegawai Pematuhan	Memastikan keselarasan amalan pembangunan dengan peraturan dan piawaian keselamatan.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 3/6
		No. Semakan: 09
		No. Isu: 01
	POLISI PENGURUSAN KOD SUMBER	Tarikh: 31/01/2023

4. TEMINOLOGI DAN SINGKATAN

PTPKM	:	Pusat Teknologi dan Pengurusan Kriptologi Malaysia
KS	:	Ketua Seksyen yang bertugas di Seksyen iDEC yang dipertanggungjawabkan
Pembekal	:	Pembekal sah yang dilantik oleh iDEC untuk kerja-kerja perkhidmatan dan penyelenggaraan
PYB	:	Pekerja Yang Bertanggungjawab
Pekerja ICT	:	Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera/Juruteknik Komputer/Pekerja lain yang dilantik untuk mengurus ICT
Pentadbir Sistem	:	Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera/Juruteknik Komputer/Pekerja lain yang mengurus operasi atau aktiviti berkaitan pengoperasian aplikasi, telekomunikasi serta pengurusan sistem pangkalan data Universiti.
TPKD	:	Timbalan Pegawai Kawalan Dokumen
TWP	:	Timbalan Wakil Pengurusan
WP	:	Wakil Pengurusan
PQC	:	Kriptografi Pasca-Kuantum
SDLC	:	<i>Software Development Life Cycle</i>
SAST	:	<i>Static Application Security Testing</i>
DAST	:	<i>Dynamic Application Security Testing</i>
IAST	:	<i>Interactive Application Security Testing</i>
KPS	:	Kod Pengurusan Selamat
SQL	:	<i>Structured Query Language</i>
XSS	:	Skrip Rentas Tapak

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 4/6
		No. Semakan: 09
		No. Isu: 01
	POLISI PENGURUSAN KOD SUMBER	Tarikh: 31/01/2023

5. RISIKO YANG BERKAITAN DENGAN KESELAMATAN KOD

- Kod yang mengandungi kelemahan keselamatan boleh dimanipulasi pihak ketiga.
- Serangan siber seperti *SQL Injection*, *XSS*, dan serangan kawalan sesi.
- Peningkatan kos pemulihan dan risiko kehilangan data jika kelemahan tidak dikesan awal.
- Ketidakpatuhan kepada piawaian keselamatan maklumat dan peraturan perlindungan data.
- Kerosakan reputasi organisasi akibat kebocoran maklumat atau gangguan operasi.


6. PELAKSANAAN SEMAKAN KOD

6.1. KEKERAPAN SEMAKAN

- Semua kod yang baru dibangunkan atau dikemas kini perlu menjalani sekurang-kurangnya satu semakan kod sebelum dihantar ke persekitaran produksi. Semakan berkala hendaklah dijalankan setiap kali perubahan kod berlaku atau sekurang-kurangnya setiap **tiga bulan**.

6.2. KAEDAH SEMAKAN

- Semua kod hendaklah disemak oleh sekurang-kurangnya seorang pembangun lain.
- Gunakan alat SAST, DAST, dan/atau IAST bagi mengesan kelemahan secara automatik.
- Kod yang menangani pengesahan, akses, penyulitan dan logik kritikal hendaklah diberi keutamaan dalam semakan keselamatan.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 5/6
		No. Semakan: 09
		No. Isu: 01
	POLISI PENGURUSAN KOD SUMBER	Tarikh: 31/01/2023

6.3. DOKUMENTASI SEMAKAN

- Semua hasil semakan hendaklah didokumenkan, termasuk nama penyemak, tarikh semakan, isu yang dikenal pasti, dan tindakan pembetulan.
- Rekod disimpan sekurang-kurangnya selama 12 bulan bagi tujuan audit dalaman dan luaran.

6.4. PENGKODAN SELAMAT


- Gunakan validasi *input* yang ketat dan pengkodan *output* untuk mengelakkan serangan suntikan.
- Elakkan penggunaan fungsi tidak selamat (seperti *strcpy* dalam C/C++).
- Pastikan semua komunikasi dan penyimpanan data menggunakan penyulitan yang diluluskan PTPKM.
- Gunakan prinsip *least privilege* dan *defense in depth* dalam pengurusan kawalan akses.

6.5. PENYULITAN DAN PENGESAHAN

Semua algoritma kriptografi mestilah berdasarkan piawaian yang ditetapkan oleh PTPKM.

6.6. LATIHAN DAN KOMPETENSI

- Semua pembangun perlu menghadiri latihan pengkodan selamat pada setiap tahun.
- Latihan *onboarding* untuk pembangun baharu mesti merangkumi pengenalan kepada dasar ini.
- Sijil latihan perlu dikemukakan kepada HR dan dikemas kini setiap tahun.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 6/6
		No. Semakan: 09
		No. Isu: 01
	POLISI PENGURUSAN KOD SUMBER	Tarikh: 31/01/2023

7. PEMATUHAN DAN PIAWAIAN

7.1. Audit Berkala

Audit dalaman akan dilaksanakan secara berkala (cth: tahunan atau separuh tahunan) bagi memastikan pematuhan terhadap polisi ini. Audit akan merangkumi aspek pelaksanaan semakan kod.

7.2. Latihan

Kakitangan yang berkaitan mesti menjalani latihan berkala mengenai amalan terbaik pengurusan dan pelaksanaan semakan kod, tanggungjawab peranan dan prosedur semakan kod. Latihan ini juga perlu dimasukkan dalam proses pengambilan staf baru dalam bidang keselamatan IT, dan dikemaskini selaras dengan perubahan dasar atau peraturan.

8. SEMAKAN DAN KEMASKINI POLISI

Polisi ini akan disemak **sekurang-kurangnya sekali setahun** atau apabila berlaku perubahan ketara dalam teknologi, peraturan atau sistem dalaman. Sebarang perubahan yang diluluskan mesti dimaklumkan kepada semua pihak yang berkaitan dan didokumentasikan secara rasmi.

9. LAMPIRAN