	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI PEMBANGUNAN MAKLUMAT DAN MALAYSIA Kod Dokumen: UPM/	Halaman: 1/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023


1. SKOP

Polisi ini merangkumi aspek pelaksanaan pembangunan sistem atau aplikasi di dalam PTPKM, termasuk pembangunan dalaman, sistem pihak ketiga (*third-party system*), pembangunan luar, dan aplikasi berdasarkan *cloud (cloud-based)*. Polisi ini terpakai kepada semua pekerja, kontraktor, dan pihak ketiga yang terlibat dalam pembangunan sistem. Semua kod mesti mematuhi prinsip yang digariskan di dalam Polisi Pengurusan Kod Sumber dan Pelan Pemulihan Bencana (*Disaster Recovery Plan, DRP*) dan Sandaran Penduaan (*Backup*).

2. TANGGUNGJAWAB


Polisi ini terpakai kepada Pentadbir IT, Pegawai Keselamatan Maklumat, Pembangun sistem, dan kakitangan yang terlibat dalam keselamatan sistem atau rangkaian. Ia juga terpakai kepada pasukan audit dalaman dan pihak pengurusan yang bertanggungjawab untuk perlindungan data dan mitigasi risiko.

Peranan	Tanggungjawab
Pembangun Sistem	Melaksanakan kod yang selamat dan mengikut garis panduan SSDLC
Pasukan Keselamatan	Menilai kawalan keselamatan
	Menjalankan penilaian risiko dan ujian keselamatan
Pengurus Projek	Memastikan semua peringkat SSDLC dipatuhi dan didokumentasikan
Operasi IT	Menguruskan penerapan dan tugas penyelenggaraan dengan selamat.
Audit Dalaman	Memantau pematuhan terhadap dasar ini dan amalan terbaik SDLC

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 3/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

4. TERMINOLOGI 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
SSDLC	:	<i>Secure Software Life Cycle</i>
UAT	:	<i>User Acceptance Testing</i>
PDPA	:	<i>Personal Data Protection Act</i>
NIST	:	<i>National Institute of Standards and Technology</i>
ISO/IEC	:	<i>International Organization for Standardization/International Electrotechnical Commission</i>
COTS	:	<i>Commercial Off-The-Shelf</i>
RBAC	:	<i>Role-Based Access Control</i>
OWASP	:	<i>Open Worldwide Application Security Project</i>
ITIL	:	<i>Information Technology Infrastructure Library</i>

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 4/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

5. PEMBANGUNAN, PENGUJIAN DAN PEYELENGGARAAN SISTEM

5.1. Pembangunan Sistem

- Aktiviti projek pembangunan sistem perlu merangkumi perkara berikut:
 - Permulaan/Definisi Projek (*Project Initiation/Definition*)
 - Penilaian Risiko (*Risk Assessment*)
 - Pengenalpastian Keperluan Pengguna (Fungsi dan Bukan Fungsi) (*Identification of Functional and Non-functional User Requirements*)
 - Reka Bentuk Sistem (*Systems Design*)
 - Pembangunan Sistem (*System Development*)
 - Jaminan Kualiti (*Quality Assurance*)
 - Dokumentasi dan Latihan (*Documentation and Training*)
 - Ujian dan Penerimaan Sistem (*Systems Testing and Acceptance*)
 - Pelaksanaan (*Deployment*)
 - Penyelenggaraan (*Maintenance*)
- Semua sistem *COTS* dan aplikasi *custom* mesti melaksanakan kawalan akses berasaskan peranan (**RBAC**). Pentadbir akses mesti menguruskan keistimewaan dan jika mereka juga pengguna, akaun berasingan untuk pentadbiran dan penggunaan hendaklah disediakan.
- Projek mesti merangkumi keperluan keselamatan yang jelas dari fasa perancangan (*planning*) hingga ke pelaksanaan (*deployment*).
- Kod sumber (*source code*) perlu dikawal versi (*version-controlled*) dan


	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 5/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

disimpan dengan selamat di dalam repositori yang sah bagi mengelakkan akses dan pengubahsuaian tanpa kebenaran.

- Semua komponen/perpustakaan pihak ketiga (*third-party libraries*) mesti dinilai untuk kerentanan (*vulnerabilities*) sebelum diintegrasikan.
- Persekitaran pengeluaran, pembangunan, dan ujian mesti dipisahkan secara logik. Semua ujian di persekitaran pengeluaran mesti menggunakan data yang telah dinyahidentifikasi (*sanitized*).

2.2 Ujian Sistem (*System Testing*)

- Semua sistem mesti menjalankan beberapa peringkat ujian, termasuk:
 - Ujian Unit
 - Ujian Integrasi
 - Ujian Sistem
 - Ujian Penerimaan Pengguna (UAT)
 - Ujian Keselamatan (termasuk analisis statik/dinamik dan penilaian kerentanan (*vulnerability assessment*)).
- Ujian hendaklah dijalankan dalam persekitaran yang terasing dan terkawal yang meneyrupai keadaan pengeluaran, tanpa melibatkan data sebenar atau sensitif.
- Laluan akses aplikasi bukan produksi (*Non-production application access paths*) mesti dipadam atau dinyahaktifkan.
- *Debugging code*, ID pengguna ujian dan kata laluan mesti dikeluarkan sebelum *deployment* selaras dengan **Garis Panduan Penyebaran Selamat (*Secure Deployment Guidelines*) OWASP dan NIST SP XXXX-XXX**.
- Semua kod sebelum pelancaran mesti disemak oleh individu selain penulis asal dan oleh mereka yang mahir dalam teknik dan amalan semakan kod, seperti yang digariskan dalam Polisi Semakan Kod/Kod Selamat.
- Semakan kod dan ujian kes penggunaan mesti dilakukan oleh pegawai


	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 6/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

dalam yang layak atau pihak ketiga yang dilantik seperti dinyatakan dalam Polisi Semakan Kod/Kod Selamat.

- Ujian mesti didokumentasikan, boleh diulang dan dilaksanakan dalam persekitaran yang terkawal.
- Log ujian mesti disimpan dengan selamat dan hanya boleh diakses oleh pihak yang dibenarkan.
- Sebarang kerentanan (*vulnerabilities*) yang dikenal pasti mesti diselesaikan sebelum pelaksanaan kepada produksi (*production deployment*).
- Ujian penembusan (*penetration testing*) mesti dijalankan sebelum pelancaran rasmi.
- Kakitangan pembangunan dan sistem mesti mengikut jadual pelancaran yang diluluskan oleh pentadbir.

2.3 Penyelenggaraan Sistem (*System Maintenance*)

- *Patching* dan kemas kini yang berkala mesti dijadualkan untuk menangani kerentanan keselamatan (*security vulnerabilities*) dan penambahbaikan sistem.
- Penyelenggaraan sistem hendaklah mematuhi Proses Pengurusan Perubahan yang formal berdasarkan **amalan terbaik ITIL dan standard ISO/IEC XXXXX**.
- Prosedur pengurusan perubahan mesti diikuti untuk semua kemas kini dan penambahbaikan.
- Akses istimewa yang digunakan semasa penyelenggaraan hendaklah dikawal rapi, dihadkan tempohnya, dan diaudit selaras dengan standard **ISO/IEC XXXXX**.
- Aktiviti penyelenggaraan mesti dipantau dan direkodkan, serta hanya dibenarkan oleh kakitangan yang dilantik.
- Pelan pengunduran (*rollback*) mesti disediakan sekiranya berlaku risiko atau kegagalan baru selepas penyelenggaraan, selaras dengan Pelan Pemulihan Bencana, Sandaran dan Keterlangsungan Perniagaan (*Disaster Recovery*,


	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 7/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

Backup and Business Continuity Plan).

- Sistem mesti dipantau selepas penyelenggaraan untuk mengenal pasti sebarang aktiviti atau isu prestasi (*performance*) yang tidak normal.
- Sistem lama (*legacy*) mesti dinilai secara berkala dari sudut pematuhan terhadap keperluan keselamatan dan tahap sokongan teknikal (*supportability*). Sistem yang tidak lagi diperlukan mesti dinyahaktifkan dengan selamat.

2.4 Dokumentasi (*Documentation*)

- Semua fasa SDLC mesti didokumentasikan dan disimpan dengan selamat.
- Keputusan penting, kelulusan, dan perubahan mesti boleh dijejaki untuk tujuan audit dan pematuhan.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 8/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

3.0 PEMATUHAN DAN PEMANTAUAN

3.1 Audit Berkala

Audit dalaman akan dijalankan secara berkala untuk memastikan pematuhan terhadap proses SSDLC dan piawaian yang berkenaan seperti PDPA, NIST, dan ISO/IEC XXXXX. Audit ini akan memfokuskan pada amalan pembangunan, ujian dan penyelenggaraan sistem.


Kegagalan untuk mematuhi akan mengakibatkan tindakan pembetulan yang mungkin melibatkan tindakan disiplin. Semua aktiviti yang berkaitan dengan pembangunan, ujian, dan penyelenggaraan mesti mematuhi dasar keselamatan organisasi, termasuk kawalan akses, perlindungan data, dan piawaian pengkodan yang selamat. Penilaian keselamatan yang berkala, termasuk imbasan kerentanan (*vulnerability scanning*) dan penilaian risiko, juga akan dijalankan secara berkala.


3.2 Latihan


Semua kakitangan yang terlibat dalam pembangunan, ujian atau penyelenggaraan mesti menerima latihan berkala mengenai amalan pengkodan yang selamat, prinsip SSDLC dan keperluan pematuhan yang berkaitan .

4.0 SEMAKAN DAN KEMASKINI DASAR

Dasar ini akan disemak semula setiap tahun atau apabila perubahan besar berlaku dalam teknologi, peraturan, atau sistem dalaman. Pasukan Keselamatan Maklumat akan mengemukakan cadangan kemaskini, yang mesti diluluskan dan dikomunikasikan kepada semua pasukan yang terlibat.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 9/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 10/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 11/11
		No. Semakan: 09
		No. Isu: 01
	POLISI PEMBANGUNAN, PENYELENGGARAAN DAN PENGUJIAN SISTEM ICT	Tarikh: 31/01/2023

5.0 LAMPIRAN