	JSC «Kazakh University of Technology and Business named after K. Kulazhanov»
	QUALITY MANAGEMENT SYSTEM
	Documented procedure

APPROVED
Rector
JSC «KazUTB named after K. Kulazhanov»
_____ L.K. Baibolova
5 October 2026

PROCESS CHANGE MANAGEMENT
KazUTB-DSD-DP-6.3-2026-13

Astana, 2026

Version: 1.0	**CI: QMSD**	**Registration №_____ on EDM**

FOREWORD

This documented procedure (DP) has been developed by the Strategic Development Department of JSC «KazUTB named after K. Kulazhanov».

This DP has been developed to ensure the registration and controlled implementation of organizational, process-related, technological, and documentation changes.

This DP shall be approved by the Rector by means of a personal signature on the title page.

This DP is mandatory for all structural departments of JSC «KazUTB named after K. Kulazhanov» insofar as their activities relate to the Quality Management System (QMS).

This DP shall be periodically reviewed by the Director of the Strategic Development Department at least once every three years.

Amendments to this DP shall be introduced based on the results of its application at JSC «KazUTB named after K. Kulazhanov» or in response to changes in applicable requirements.

This DP has been developed and is being implemented for the first time at JSC «KazUTB named after K. Kulazhanov».

CONTENT

1. Terms and definitions 4
2. General provisions 5
3. Principles of change management 5
4. Roles and responsibilities 6
5. Classification of changes 7
6. Change management procedure 8
7. Monitoring and evaluation of performance 12
8. Records and privacy management 13
9. Risks associated with the process and actions to prevent risks 14
10. Final provisions 14
Applications 15
Assessment of the impact and risks of change 16
Change implementation plan 18
Register of changes 19
Evaluate performance and close change 20

1. TERMS AND DEFINITIONS

The term	Definitions
Change	A planned or emergency transformation of a process, system, structure, document, resource, technology, or way of working.
Initiator	The employee, department, collegial body or project team that submitted the change request.
Change Owner	The person responsible for justifying, planning, coordinating
Process owner	An official responsible for the performance of the process and the resources and risks associated with it.
SDD	Strategic Development Department.
DDaITD	Department of Digital Development and Information Technology
Dependencies	Works to be completed before the start of other works
IS	Information security.
Change	A planned or emergency transformation of a process, system, structure, document, resource, technology, or way of working.
Cybersecurity	The state of protection of electronic information resources of information systems and infrastructure from threats in the digital environment.
Checkpoints	Steps in which progress is checked
Communications	Ways of informing the public
Completion Criteria	Signs that contributed to the successful implementation of the change
Events	Actions to be performed
Data migration	Data to be migrated to the new system or format
Responsible	Those who perform and control every action
Rollback	Reverting to a previous working state if critical errors, failures, or unacceptable consequences occurred after implementation. For example, restoring a previous version of a system or document.
Impact Assessment	Identify the possible consequences for the goals of processes, people, resources, data systems, and mandatory requirements.
Pilot	Trial implementation of a change in a limited area: in one department, system, group of users, or during a certain period. A pilot allows you to test a change before it is fully implemented.
Personal data	Information relating to a specific or identifiable personal data subject.
Rollback plan	Planning for the previous state, in cases of failed implementation
Implementation plan	List of activities, sequence and interconnection of work, responsible persons, deadlines, resources, control points, procedure for checking the results, training and informing employees, transferring and backing up data, returning to the previous state in case of unsuccessful implementation, as well as criteria for successful completion of the change.

Testing	Verify that the change is working correctly, meets the requirements, and does not cause errors or negative impacts on other processes and systems.
Emergency Change	A change that must be implemented without going through the full standard cycle before implementation to prevent or limit significant damage.

2. GENERAL PROVISIONS AND PROCEDURE DESCRIPTION

2.1 This documented procedure establishes a unified process for initiating, assessing, coordinating, approving, implementing, monitoring, and closing changes that may affect the objectives of JSC «KazUTB named after K. Kulazhanov», the quality of educational and other services, management system processes, information assets, personal data, anti-corruption measures, resources, and obligations to interested parties.

2.2 This procedure applies to all structural subdivisions, collegial bodies, project teams, and process owners of JSC «KazUTB named after K. Kulazhanov».

2.3 This procedure covers both planned and emergency changes, including changes to:

2.3.1 Organizational structure, distribution of authority and responsibilities;

2.3.2 Strategy, policies, objectives, performance indicators, and plans;

2.3.3 Educational, administrative, research, and support processes;

2.3.4 Information systems, software, infrastructure, integrations, and access rights;

2.3.5 Categories, purposes, methods, retention periods, and locations of personal data processing;

2.3.6 Documented information, record forms, and approval workflows;

2.3.7 External suppliers, contractors, cloud services, and other third parties;

2.3.8 Anti-corruption measures, control procedures, and mechanisms for reporting violations.

2.4 Editorial corrections that do not alter requirements, responsibilities, process workflows, data composition, or control measures shall be handled in accordance with the established procedure for the control of documented information. If an editorial change may affect process execution, information security, personal data, or compliance with mandatory requirements, it shall be managed in accordance with this procedure.

2.5 The purpose of this procedure is to ensure that every significant change is justified, assessed prior to implementation, provided with the necessary resources, agreed upon by authorized personnel of JSC «KazUTB named after K. Kulazhanov», implemented in a controlled manner, and evaluated based on its results.

3. PRINCIPLES OF PROCESS CHANGE MANAGEMENT

3.1 The practical requirement for the principle of change management is given in the table:

Principle	Practical requirement
Validity	Change has a clear goal, problem, expected result, and measurable criteria for success.
Proportionality	The depth of the assessment and the level of approval are appropriate for the scale of the risk and impact.
Preliminary assessment	Risks, resources, dependencies, and prerequisites are evaluated prior to implementation.
Security by default	Cybersecurity and personal data protection are built into the solution at the design stage.

Principle	Practical requirement
Prevention of corruption risks	The change must not create opaque authority, conflict of interest, circumvention of control, or unfair advantage.
Traceability	Decisions, approval of the test version, deviations and results are recorded.
Managed implementation	Critical deadlines, communication resources, training, and a rollback plan are assigned.
Checking the result	The change is closed only after the implementation is confirmed and the effectiveness is evaluated.

4. ROLES AND RESPONSIBILITIES

4.1 Roles and responsibilities are distributed in the table:

Role	Responsibility
President or Rector	Approves high and critical level changes within the scope of authority, makes decisions on resources and acceptable residual risk.
SDD	Owns the change management methodology, registers significant changes, checks the completeness of the assessment, coordinates inter-process approval, maintains a consolidated register and monitoring. The SDD is the developer and owner of the methodology of the University's Anti-Corruption Policy and assesses the compliance of changes with its requirements.
Process owner	Accepts or initiates a change, assigns a change owner, and provides resources, alignment, execution, and evaluation of the outcome in its process.
Change Owner	Prepares an application and impact assessment, forms a plan, organizes testing, communication, implementation, monitoring, rollback, if necessary, and a closure report.
DDaITD	Assesses architecture, access, vulnerabilities, logs, backups, integration resilience, and vendor risks, aligns digital changes, and monitors technical readiness.
Data Protection Officer	Checks the lawfulness of the purpose, minimization of data, the rights of subjects, access, transfer, storage, deletion and the need for a privacy impact assessment.
Legal support	Reviews applicable legal, contractual and regulatory requirements, including the terms of interaction with third parties.
Finance Division	Confirms budget and economic impact when a change requires funding or changes financial control procedures.
HRD and heads of SD	Competencies, workload, training, changes in job responsibilities and informing employees are assessed.

Role	Responsibility
Internal audit	Independently assesses compliance with the procedure and the effectiveness of control measures in accordance with the audit program.
Workers and users	Follow the approved procedure, participate in training, report deviations, incidents and unforeseen consequences.

4.2 The development of the Anti-Corruption Policy by the SDD does not give the authority to investigate possible corruption offenses.

4.3 Reports and inspections are considered by authorized persons in accordance with the established procedure.

5. CLASSIFICATION OF CHANGES

5.1 Types of changes:

Type	Examples
Organizational	Structure, powers, staff, distribution of functions, collegial bodies
Process	Stages, inputs, outputs, metrics, interaction milestones
Digital & Infrastructure	Integration systems, equipment, networks, cloud services, access rights
Data & Privacy	New categories of data: purposes of questionnaire processing, analytics, transfer, storage, deletion
Documentaries	Policies, procedures, forms, records, classifiers, routes, and versions
Regulatory	Changes in laws, standards, licenses, accreditation and contractual requirements
Financial and Procurement	Budget, Rates, Purchases, Payments, Donations, Suppliers and Separation of Responsibilities
Emergency	Remediate a critical vulnerability, disaster, failure, security threat, or mandatory violation

5.2 ***Levels of significance:***

Level	Criteria	Approval
Low	Local reversible change without affecting the objectives of the process, access rights, personal data and mandatory requirements.	The process owner.
Medium	Change a single process or business unit with limited impact on users, resources, documents, or metrics.	The owner of the process after the DSM and the affected features have been reconciled.

Level	Criteria	Approval
High	Inter-process change: significant digitalization, transfer of data to third parties, significant costs, change of authority, or high risk.	The President or the Rector within the powers after mandatory approvals.
Critical	The possibility of a violation of the law, a significant information security incident, mass impact on personal data subjects, the suspension of a key process, or significant reputational damage.	President or Rector. Unacceptable risks must be eliminated or reduced before implementation.

5.3 ***Risk assessment:***

5.3.1 Risk is assessed as the product of the probability and severity of consequences on a scale from 1 to 5. The final score is used as a guideline and does not replace the professional opinion of the relevant department.

Score	Level	Solution
1–4	Low	Implementation of standard control measures.
5–9	Moderate	Assign additional measures and control the process owner.
10–16	High	Risk mitigation plan, mandatory profile coordination and enhanced monitoring.
17–25	Critical	Implementation is prohibited until the risk is reduced or a special decision of the authorized manager, if it is allowed by law and internal requirements.

6. CHANGE MANAGEMENT PROCEDURE

6.1 ***Change Management Procedure***:

Stage	Action	Exit	Responsible
1	Initiation	Application for change in the form **F.SDD-DP-6.3-2026-13-01**	Initiator
2	Pre-check and registration	Record number, category, and approval route	DSM or Process Owner
3	Impact and Risk Assessment	Form **F.SDD-DP-6.3-2026-13-02** conclusions of profile functions	Change Owner
4	Coordination and approval	Decision to implement, rework, pilot or reject	Authorized persons
5	Planning	Implementation Plan Form **F.SDD-DP-6.3-2026-13-03**	Change Owner
6	Testing and Readiness	Test results, backups, training, and rollback plan	Executives and Core Functions
7	Implementation	Completed activities, recordings and communications	Change Owner

Stage	Action	Exit	Responsible
8	Monitoring and closure	Evaluation of the result Form **F.SDD-DP-6.3-2026-13-05** and updated register in the form **F.SDD-DP-6.3-2026-13-04**	Process Owner and SDD

6.2 ***Initiation:***

6.2.1 The initiator shall complete a change request on Form **F.SDD -DP-6.3-2026-13-01**. The application shall contain a problem or opportunity, expected outcome, processes and systems affected, tentative timelines, resources, known risks, and success criteria.

6.2.2 The grounds may be the strategy and goals, the results of the audit and analysis of the management, non-conformities, requests from stakeholders, changes in legislation and standards, incidents, information security threats, the need to protect personal data, technological development or proposals for improvement.

6.3 ***Pre-check and registration:***

6.3.1 The Process Owner, together with the SDD, checks the completeness of the application, the absence of duplication, compliance with the strategy and the need to apply this procedure. A significant change is registered in the Register of Changes in the Form **F.SDD -DP-6.3-2026-13-04** with the assignment of a unique number.

6.3.2 At this stage, the owner of the change, the preliminary level of significance, mandatory approvers and the need for piloting are determined. An incomplete application is returned to the initiator with a list of required additions.

6.4 ***Comprehensive impact and risk assessment:***

6.4.1 The owner of the change organizes an assessment in accordance with the Form **F.SDD -DP-6.3-2026-13-02**. The analysis is carried out in an amount commensurate with the significance and covers at least the following areas:

- strategic goals, quality of services and stakeholder satisfaction;
- Process interactions, metrics, milestones, and documented information
- authority, division of duties, competencies, workload and training;
- financing, procurement, contracts, suppliers and business continuity;
- information security, cyber resilience, architecture, access, and event logs;
- personal data, data subject rights, cross-border or external transfers and retention periods;
- anti-corruption risks, conflict of interest, transparency of decisions and control of operations;
- legal, environmental, protective, reputational and other applicable consequences.

6.5 ***Mandatory Cybersecurity Assessment:***

6.5.1 The DD&ITD is mandatory if the change affects the information system, network, integration, account, access rights, authentication tool, remote access, cloud service, IT provider, electronic information resource or backup.

6.5.2 Prior to agreement, the following should be determined:

- information assets and their owners, the required levels of confidentiality, integrity and availability;
- Vulnerability threats and failure scenarios, including vendor dependency
- roles and minimum necessary access rights, the procedure for their issuance, revision and revocation;
- Requirements for authentication, encryption, logging, monitoring, updates, and backups
- security testing plan, acceptance criteria, incident response and rollback procedure;
- separating the test and production environments and prohibiting the use of real personal data in tests without justification and protection.

6.5.3 A change may not be implemented if there is an unpatched critical vulnerability, no necessary backups or recovery plan, undefined privileged access, or no mandatory opinion from the relevant department.

6.6 ***Mandatory Personal Data Protection Assessment:***

6.6.1 An assessment shall be carried out prior to implementation if the change introduces a new purpose or method of processing, a new category of subjects or data, automated decision-making, aggregation of data sets, video surveillance, biometrics, mass questionnaires, external or cloud service, transfer to a third party, or a change in the storage period and location.

6.6.2 The person responsible for personal data and the Department of Defence and Vocational Education shall check:

- the existence of a legal basis and a specific purpose of processing;
- proportionality and minimization of the composition of data;
- the procedure for obtaining consent, when it is required and confirmation of informing the subject;
- access restriction, confidentiality, registration of actions and obligations of processors;
- location, retention periods, archiving, anonymization and safe destruction;
- transfers to third parties and contractual claims against the processor;
- exercising the rights of subjects and the procedure for responding to personal data security breaches.

6.6.3 For a change with a high risk to the rights and legitimate interests of the subjects, an extended assessment of the impact on the protection of personal data is drawn up as an appendix to the Form **F.SDD -DP-6.3-2026-13-02**. Until the unacceptable risk is eliminated, processing does not begin.

6.7 ***Assessment of anti-corruption impact:***

6.7.1 The DSM, as the developer of the Anti-Corruption Policy, verifies the consistency of the change with the established principles and control measures. If necessary, the Department of Defence Management, Procurement, Procurement and Compliance Officer and an authorized person of the Compliance Officer are involved.

6.7.2 The following shall be checked during the evaluation:

- conflict of interest and affiliation of decision-makers;
- concentration of incompatible powers and the possibility of circumvention of approval;
- transparency of criteria for selection, admission, allocation of resources and decision-making;
- risks in procurement, donations, gifts, entertainment expenses, intermediaries and counterparties;
- traceability of the decision, preservation of records and availability of a channel for reporting violations;
- the need for additional verification of the counterparty and special contractual conditions.

6.7.3 The presence of an unresolved conflict of interest, non-transparent exclusion from the established procedure or the inability to ensure the division of key powers is the basis for the suspension of approval.

6.8 ***Coordination and approval:***

6.8.1 The approval route is formed according to the actual impact of the change, and not only according to the initiator's department. The approving person confirms the scope of his competence and records comments, conditions or refusal.

Condition	Mandatory approval
Significant change	Process Owner and SDD
Information Systems and Cybersecurity	DDaITD and SDD
Personal data	Responsible for Personal Data and CaLSO
Procurement budget, contracts	PAaAD, Procurement and Supply Department, CaLSO by applicability
Powers, staff, training	HRO and heads of affected units
Anti-corruption measures	SDD, CaLSO and other authorized functions on applicability
High or critical level	The President or the Rector in accordance with the powers of the

6.8.2 A decision can have one of the following statuses: approved; approved with conditions; sent to the pilot; returned for revision; postponed; rejected.

6.8.3 The conditions and deadlines for their implementation are included in the implementation plan.

6.9 ***Planning and preparation of implementation:***

6.9.1 After approval, the change owner forms an Implementation Plan according to the Form **F.SDD-DP-6.3-2026-13-03**. The plan includes activities, dependencies, responsible persons, deadlines, resources, checkpoints, testing, training, communications, data migration, backup, rollback plan and completion criteria.

6.9.2 Prior to launch, the change owner confirms that documentation, personnel, infrastructure, contracts, hardware, and support channels are ready. For high and critical changes, a readiness meeting is held with a solution.

6.10 ***Testing and piloting:***

6.10.1 If the change can be safely verified on a limited scale, a pilot is conducted. Pilot conditions, sampling, timing, success and termination criteria are determined in advance. Test results and identified deviations are documented.

6.10.2 Testing should confirm both the functional result and the operability of control measures. For digital changes, access, security, recovery, integrations, load, event logs, and correctness of data processing are checked separately.

6.11 ***Implementation and Communications:***

6.11.1 The change is implemented in the approved window and according to the plan. Deviation from the approved scope, timeline, or architecture requires a reassessment of the changed impact.

6.11.2 Affected employees and users are informed about the purpose, date, new responsibilities, available support and actions in case of deviations before the change comes into force. Training and familiarization are recorded in the prescribed form.

6.12 ***Monitoring, assessment and closure:***

6.12.1 After implementation, the change owner monitors the performance during the established stabilization period. Baseline and target status, actual results, incidents, cases, incremental costs, and residual risks are compared.

6.12.2 The change is closed according to the Form **F.SDD-DP-6.3-2026-13-05** after confirmation that:

- the success criteria have been achieved or the rejections have been accepted by an authorized person;
- unforeseen consequences are eliminated or included in a separate action plan;
- documents, registers, access rights, contracts and training materials are updated;
- temporary accesses and test data are deleted or brought to an approved mode;
- residual risks are assessed and accepted by the process owner;
- The results and lessons learned are included in the register.

6.12.3 If the result is not achieved or the risk exceeds the acceptable level, the process owner decides on corrective actions, additional monitoring, partial rollback or full return to a steady state.

6.13 ***Emergency Changes:***

6.13.1 An emergency procedure applies only to prevent or limit significant damage, eliminate a critical vulnerability, restore a key service, fulfill an urgent mandatory requirement, or respond to an incident.

6.13.2 Prior to implementation, as far as possible, the cause, owner, affected assets, minimum risk assessment, backup copy or other method of recovery, authorization of the authorized person and verification plan are recorded. Urgency does not override legal requirements, personal data protection and minimum necessary information security measures.

6.13.3 No later than the next working day, the change shall be registered, and within five working days a full analysis shall be carried out, an assessment of the result shall be drawn up and a decision shall be made on preservation, revision or rollback. If a stricter deadline is established by internal acts, it shall be applied.

6.14***Grounds for suspension or refusal:***

- there is no legal basis or the change contradicts the mandatory requirement;
- The owner, resources, success criteria, or rollback plan are not defined.
- mandatory assessment of information security or personal data protection has not been carried out;
- unacceptable critical risk remains;
- the conflict of interest has not been resolved or the necessary division of powers is lacking;
- test results do not confirm readiness;
- the conditions of the previous agreement have not been met.

7. MONITORING AND EVALUATION OF PERFORMANCE

7.1 At least once a year, the DSS analyzes the Register of Changes and submits summary information to the management as part of the established reporting of the management system. The frequency may be increased taking into account the number and risk of changes.

7.2 ***Performance evaluation indicators:***

Indicator	Approach to calculation
Percentage of changes completed within the approved deadline	Number of changes closed in time to the total number of closed changes
Percentage of effective changes	Number of Changes Achieving Success Criteria to Number of Evaluated Changes

Indicator	Approach to calculation
Proportion of emergency changes	Number of Emergency Changes to Total Number of Implemented Changes
Post-implementation incidents	Number of incidents and significant deviations related to changes
Completeness of mandatory grades	Proportion of digital and data-related changes with required conclusions
Activity Closure Deadline	Percentage of corrective actions completed within the prescribed time frame

7.3 Target values are set annually, taking into account the strategy, maturity of processes and results of the previous period. Negative dynamics are the basis for analyzing the causes and corrective actions.

8. RECORDS AND PRIVACY MANAGEMENT

Recording	Responsible	Storage	Term
Change request	Change Owner and SDD	Document management system or approved repository	By the nomenclature of cases and applicable requirements
Impact Assessment and Conclusions	Change Owner and Profile Features	Limited access by need to know	By the nomenclature of cases and applicable requirements
Implementation plan and test results	Change Owner	Project or process storage	By nomenclature of cases
Register of changes	SDD	Centralized storage	Constantly updated
Evaluation of the result and decision to close	Process Owner and SDD	Document Management System	By nomenclature of cases
Approval and familiarization sheets	Document or process owner	Document Management System	By nomenclature of cases

8.1 Records containing personal data, restricted information, security configurations, vulnerabilities or inspection materials are labeled and protected according to their category. Access is granted only to persons who need it to perform their duties.

8.2 In the preparation of reports, anonymized and aggregated information is used, if disclosure of identifying information is not required. Destruction of records is carried out in a secure way with fixation, when it is provided for by internal procedures.

9. RISKS ASSOCIATED WITH THE PROCESS AND ACTIONS TO PREVENT RISKS

9.1 Risks associated with:	9.2 Risk Prevention Actions:
– The change is initiated without sufficient justification or with incomplete data; – The significance of the change and the route of approval are incorrectly determined. – Disruption of business continuity during implementation. – Cyber incident, vulnerability or unauthorized access. – Violation of personal data requirements. – Corruption risk or conflict of interest. – Loss of traceability of decisions and uncontrolled expansion of volume.	– Check the completeness of the Form **F.DSR-DP-6.3-2026-13-01**; set the goal, expected result, resources and success criteria; return an incomplete application for revision. – Apply the criteria in Section 6; Identify the affected functions; Coordinate the route with DSM prior to implementation. – Define the deployment window, dependencies, backups, recovery and rollback plan; check support readiness in advance. – Conduct mandatory information security assessment; apply minimum rights, multi-factor authentication for applicability, logging, updates, security testing, and privileged access control. – Verify the lawful basis and purpose; Minimize data; Restrict access; Determine retention periods and deletions; Evaluate external transfers and processors. – Identify and resolve conflicts of interest; Divide incompatible powers; Ensure transparency of criteria, approvals and records; Conduct a check of the counterparty for applicability. – Record versions, decisions, and rejections. Prohibit changes to the approved scope without re-evaluation. Retain confirmation records and close temporary accesses.

10. FINAL PROVISIONS

10.1 This DP shall be enforced by an administrative document of the authorized head.

10.2 Heads of departments shall ensure that employees are familiarized and the procedure is applied within the scope of their functions.

10.3 The DSS coordinates the updating of the procedure. Proposals for change are sent to the SDD with justification and impact assessment.

10.4 Issues not regulated by the procedure shall be resolved in accordance with the legislation of the Republic of Kazakhstan, applicable standards and internal documents of JSC «KazUTB named after K. Kulazhanov».

APPLICATIONS

F. DSD-DP-6.3-2026-13-01 (mandatory)

PROCESS CHANGE REQUEST

Completed by the initiator and submitted to the process owner or SDD for registration and routing.

Field	Table of Contents
Registration number	
Date of submission	
Initiator and contacts	
Process owner	
Proposed change owner	
Name of the change	
Problem or opportunity	
Goal and expected result	
Affected processes of the system department	
Tentative deadlines	
Resources needed	
Known Risks and Limitations	
Success criteria	

Preliminary category	☐ low ☐ average ☐ high ☐ critical
Decision to review	☐ Accept ☐ Revise ☐ Reject
Signature of the process owner and date	

F.DSD-DP-6.3-2026-13-02 (mandatory)

ASSESSMENT OF THE IMPACT AND RISKS OF CHANGE

It is filled in by the owner of the change together with the relevant departments. For each applicable direction, the risk, measures and conclusion are indicated.

Scope	Influence	Risk or consequence	Control measure	Responsible
Strategy and goals	☐ Yes ☐ No			
Quality of services and users	☐ Yes ☐ No			
Processes, indicators, documents	☐ Yes ☐ No			
Structure, authority, personnel	☐ Yes ☐ No			
Procurement Budget Contracts	☐ Yes ☐ No			
Business continuity	☐ Yes ☐ No			
Information Systems and Information Security	☐ Yes ☐ No			
Personal data	☐ Yes ☐ No			
Anti-corruption risks	☐ Yes ☐ No			
Legal and Other Requirements	☐ Yes ☐ No			

Risk scale: probability of ___ out of 5 × consequences of ___ out of 5 = ___ points. Residual risk after measures: ___ points.

Parameter	**Conclusion**
Final level	☐ Low ☐ Medium ☐ High Critical ☐
A pilot is needed	☐ Yes ☐ No Justification: _____
A rollback plan is needed	☐ Yes ☐ No
Proposed solution	☐ Agree ☐ Agree with the terms ☐ Finalize ☐ Reject
Conditions and restrictions	

Approver	**Conclusion**	**Signature and Date**
Process owner		
SDD		
DDaITD		
Responsible for Personal Data and CaLSO		

F.DSD-DP-6.3-2026-13-03(mandatory)

CHANGE IMPLEMENTATION PLAN

The plan should include provisioning, testing, communication, training, migration, checkpoints, and rollback activities

Field	Table of Contents
Change number by registration number	
Process Name	
Change Owner	
Planned implementation window	
Period of enhanced monitoring	

№	Event	Result	Responsible	Term	Resource	Status

Rollback or Recovery Plan:

_____

_____

Launch readiness criteria:

_____

_____

Communication and Training Plan:

_____

F. DSD-DP-6.3-2026-13-04

REGISTER OF CHANGES

SDD is maintained. For digital changes, a system or information asset is additionally specified.

№	Date	Change	Process or system	Lv	Owner	Solution	Term	Status

Recommended statuses: registered; evaluated; approved; prepared; pilot; implemented; monitored; closed; rejected; postponed; rollback.

F.DSD-DP-6.3-2026-13-05

EVALUATE PERFORMANCE AND CLOSE THE CHANGE

It is issued at the end of the stabilization period. The decision to close is made by the owner of the process and confirmed by the DSR for the registered changes.

Field	Table of Contents
Change number and name	
Implementation date	
Follow-up period	
Planned Success Criteria	
Actual results and indicators	
Case rejection incidents	
Post-Implementation Risk Status	
Updated documents and accesses	
Lessons learned	
Unfinished actions, responsible deadlines	

Parameter	Mark
Conclusion	☐ effective ☐ partially effective ☐ ineffective
Solution	☐ Close ☐ Renew Monitoring ☐ Corrective Actions ☐ Partial Rollback ☐ Full Rollback
Process owner	Full name _____ Signature _____ date _____
SDD	Full name _____ signature _____ date _____

F. DSD-7.5-2026-01-02 (mandatory)

APPROVAL SHEET

Position	Full name	Date	Signature
Vice-Rector for AA	Askarbekov E. B	02.10.2026	
Vice-Rector for SAaSD	Berdigaliuly S.	02.10.2026	
Vice-Rector for AaIA	Orazbekov E.E.	02.10.2026	
Director of the SDD	Orazalina D. K.	02.10.2026	
Director of the DDaITD	Sauatov B.S.	02.10.2026	
Head of LAaHRD	Zaynutdinov A.A.	02.10.2026	
Head of HRO	Myrzalieva M. B	02.10.2026	
Head of the CaLSO	Kuat A.A.	02.10.2026	
Head of QMSO	Ernst A.S.	02.10.2026	

F. DSD-7.5-2026-01-03 (mandatory)

FAMILIARIZATION SHEET

Position	Full name	Date	Signature

F. DSD-7.5-2026-01-04 (mandatory)

CHANGE REGISTRATION SHEET

The number of the changed In the case of the	Change Notice Number	Number of sheets (pages)				Total sheets (after changes)	Date of submission	Full name of the person making the changes	Signature of the person who made the changes
		changed	replaced	new	cancelled				

F. DSD-7.5-2026-01-05 (mandatory)

PERIODIC INSPECTION RECORD SHEET

Verification Date	full name of the person, who performed the Verification	Signature of the person, who performed the check	Wording of comments